Liquid computing: A structured approach to identifying incremental risks and controls resulting from autonomous synchronisation

By

Alwyn Jacobus Nicolaas Visser

Assignment presented in partial fulfilment of the requirements for the degree of Master of Commerce (Computer Auditing) in the Faculty of Economic and Management Sciences at Stellenbosch University

Supervisor: Ms Anria Sophia van Zyl

March 2017

Declaration

By submitting this assignment electronically, I declare that the entirety of the work contained therein is my own, original work, that I am the sole author thereof (save to the extent explicitly otherwise stated), that reproduction and publication thereof by Stellenbosch University will not infringe any third party rights and that I have not previously in its entirety or in part submitted it for obtaining any qualification.

Alwyn Jacobus Nicolaas Visser
Date: March 2017

Abstract

The millennial generation is entering the labour market. This generation has never known any era before hyper-connectivity. They want to be constantly connected. This results in changes in the business environment. Employers allow employees to connect to networks, using their own personal mobile devices. These devices are the property of the employees and not governed by the security and other policies of the employer. Constant synchronisation of data to and from these employee-owned devices enables users of these devices to always have relevant, timeous data on their devices and to handoff computing tasks seamlessly from one device to another in a scalable computer environment. This is liquid computing.

Liquid computing results from the way users use the underlying enabling technologies. With each new technology, comes new risks. In order to understand the risks incremental to liquid computing, the components and enabling technologies of a liquid computing environment must be fully understood. A comprehensive literature study was conducted on the enabling technologies. The purpose of this study is to define liquid computing and then use an established control framework in order to identify the risks incremental to this technology. The risks are mapped to the control framework. The identified risks consist mainly of risks pertaining to the privacy and integrity of data. The risks are quantified and controls are recommended to mitigate the risks incremental to liquid computing. These controls are also quantified. The unmitigated risk remaining, after implementing mitigating controls, is calculated.

These risk and control matrixes will assist businesses in understanding and quantifying the risks related to a liquid computing environment and will help management to evaluate whether an organisation has sufficient control redundancy to address the risks.

Opsomming

Die millennial generasie begin die arbeidsmark betree. Hierdie generasie het nooit ‘n era geken voor hiper-konnektiwiteit nie. Hierdie generasie wil konstant gekonnekteer wees. Hierdie veranderende kultuur het veroorsaak dat die besigheidsomgewing verander het. Werkgewers laat hulle werknemers toe om persoonlike toestelle aan netwerke te koppel. Hierdie toestelle is die eiendom van die werknemers en word nie beheer deur die werkgewer se sekuriteits- en ander beleide nie. Konstante sinchronisasie van data na en van hierdie toestelle wat deur werknemers besit word, stel gebruikers in staat om altyd tydige, relevante data op hierdie toestelle te hê en om take sonder moeite tussen toestelle te oorhandig in ‘n rekenaaromgewing met wisselende grootte. Dit is ‘n vloeibare rekenaaromgewing.

‘n Vloeibare rekenaaromgewing is die resultaat van die manier waarop gebruikers die onderliggende tegnologieë gebruik. Saam met elke nuwe tegnologie, kom daar nuwe risiko. Die komponente, en onderliggende tegnologieë van ‘n vloeibare rekenaaromgewing moet behoorlik verstaan word, sodat die risikos inkrementeel aan ‘n vloeibare rekenaaromgewing verstaan kan word. Die onderliggende tegnologieë is bestudeer deur ‘n omvattende literatuurstudie. Die doel van hierdie studie is om ‘n vloeibare rekenaaromgewing te definieer en dan ‘n gevestigde kontroleraamwerk te gebruik om die risikos inkrementeel aan hierdie tegnologie te verstaan. Die risikos is gekoppel aan die kontroleraamwerk. Die risikos bestaan hoofsaaklik uit risikos wat verband hou met die privaatheid en integriteit van data. Die risikos is gekwantifiseer en kontroles voorgestel vir die risikos wat inkrementeel tot ‘n vloiebare rekenaaromgewing is. Hierdie kontroles is ook gekwantifiseer. Die oorblywende risiko, nadat die kontroles implementer is, is bereken.

Hierdie risiko- en kontrole matrikse sal besighede help om die risikos inkrementeel aan ‘n vloeibare rekenaaromgewing te verstaan en kwantifiseer en sal bestuur help om te beoordeel of die onderneming voldoende oortolligheid in kontroles het, om die risikos aan te spreek.

Acknowledgements

- “I will give thanks to you, Lord, with all my heart; I will tell of all your wonderful deeds.” – Psalm 9:1
- My study leader, Ms Anria van Zyl, who knew exactly how to motivate and push me to finish this. Thank you also for your guidance through the process.
- Professors Riaan Rudman and Willie Boshoff, for guidance throughout the course.
- Lindie Lucas, for all the encouragement, the food, the beverages and the cold medicine. I will never deserve you, but I promise to keep improving.
- Eduard & Tanya Visser, Juan & Elmarié Morison, Rayno Visser and other family: thank you for constant support and love.
- Each and every friend, I wish I could name all of you. You are the most valued players!
- Information systems team (and I have to single out Mr Len Steenkamp) – this one is for you. Thank you for all the laughter and making the office a place I want to be at.
- Francois Swan and Devlin Tyack, your relentless work ethic and drive inspire me to constantly push harder.
- Dale Russell – you deserve your own bullet in here. Since I have met you, you have always been the hardest worker in the room. I have so much respect for you.
- JJ Stegmann, Kirstin Mostert, Stuart Campbell-Gillies, Alex Boshoff, Chris van der Meulen, Devon Walker, Ruan van Jaarsveld – students like you fuel my fire for this University. Thank you for firing my passion!
- Three senior colleagues whom I look up to and who inspire me to be an academic – Professors Wim de Villiers, Stan du Plessis and Ronel du Preez. I am so humbled and proud to be working at this University in your era.
- Stellenbosch University – *Domus dulcis domus!*

Table of Contents

List of Figures

List of Tables

List of Abbreviations

The use of abbreviations and acronyms has generally been avoided, except where the relevant abbreviations are well known and the use of the full name would clutter the text. Abbreviations and acronyms commonly used are:

BYOD	Bring Your Own Device
COBIT	Control Objectives for Information and Related Technologies (all references to COBIT in this paper refers to COBIT Version 5)
IODSA	Institute of Directors in Southern Africa
ISO	International Standard Organisation
IT	Information Technology
ITGI	Information Technology Governance Institute
ITIL	Information Technology Infrastructure Library
SaaS	Software as a service
UWYT	Use What You are Told
WiFi	Wireless Fidelity
WiMax	Worldwide Interoperability for Microwave Access

Chapter 1 – Introduction

1.1 Background to the problem

In recent years, mobile devices such as smartphones, tablets and laptops have pervaded virtually every sphere of human existence. This trend is set to continue since the Millennial generation is starting to enter the labour market and they have never known an era without hyper-connectivity and the internet. The implications of this era on business, cannot be ignored. According to recent studies, the proliferation of mobile devices have been made possible by modern mobile operating software pushing development of powerful mobile devices and the development of a vast array of application software (Armando, Costa, Verderame & Merlo, 2014). This has led to a trend of mobility, where mobile devices are increasingly used to access the internet. Aker and Mbiti (2010) makes the case that mobile phones have switched roles from communication devices to a platform for service delivery.

The mobility trend has led to a paradigm in which employees are allowed access to company resources through their own personal mobile devices (Armando *et al.*, 2014). This paradigm is commonly referred to as “bring-your-own-device” (BYOD). Kabanda and Brown (2014) argue that Europe, Asia and America are enthusiastic about the adoption of BYOD, while developing countries do not yet fully understand the paradigm shift.

A BYOD strategy is not only convenient to the user, but it also bears a low cost to the organisation employing the policy (Imazeki, 2014). This strategy allows employees to use their own mobile devices at work, whilst reducing the capital investment required by organisations and at the same time increasing employee efficiency (Armando *et al.*, 2014). Organisations in developing countries are especially slow to invest in expensive resources and equipment and BYOD strategies will benefit these organisations, although cost to employees is a consideration that will hamper implementation in these countries (Kabanda & Brown, 2014). Some organisations supply devices, preloaded with branded applications, to their employees. The study would also

be relevant to these organisations as many of the risks will revolve around human behaviour and how the technology is used by the employees.

Kabanda and Brown (2014) argue that there are still concerns among management of corporate entities in developed countries regarding the adoption of BYOD. Using a BYOD strategy results in users downloading applications on personal devices to access and use company data. In order to access company data on mobile applications, users must grant access or permissions which is referred to as discretionary access controls, chosen by the employees, in contrast to the usually strict security measures enforced by companies over their data (Armando *et al*., 2014: 48–56).

Applications developed for use on mobile devices, often do not provide sufficient encryption and security measures to safeguard proprietary and sensitive company information. Controls on application level are thus designed, tested and implemented by application developers. Application developers concentrate on viruses and malware when taking security measurers into consideration during application development stages (Armando *et al*., 2014: 48–56). Specific policies and procedures of companies are not incorporated into off the shelf applications used to access and manipulate company data. The risk arise that personal devices can run applications that might violate organisation security policy (Armando *et al.*, 2014). The Charleston Law Review also makes the case that trade secrets and patents are vulnerable when company data is stored on employee devices who might leave the entity or the device is lost (Comisky & Diamond, 2014). Employee devices are also susceptible to hacking, cloning and theft which would increase this vulnerability.

1.2 Problem statement

The convergence of the mobility and BYOD trends, has led to an increased demand by users to be able to access company resources in order to do their work from anywhere and at any time. Navigation between multiple databases and files are inefficient and cumbersome and thus technology has evolved to synchronise information automatically between devices and networks.

The need has thus arisen for synchronisation of multiple datacentres into single applications to increase efficiency and ease of use. Liquid software is a term used for an infrastructure system that dynamically moves functionality (Hartman, Manber & Peterson, 1996). These infrastructure systems result in users allowing data to synchronise onto different applications and platforms. A device could be set up to synchronise to multiple servers while multiple devices can synchronise to and from a single cloud-based server.

A practical application would be a user who synchronises a work calendar to a personal mobile device. The work calendar would automatically be duplicated on the mobile device's local memory. If this same device is set to synchronise to another cloud-based calendar, such as Google calendar, the work calendar will also synchronise to the cloud based platform unless this is specifically disabled during setup. In a liquid state, these synchronisation sessions would schedule automatically without the user necessarily realising that the device is writing to and downloading from the cloud.

In a truly liquid computing environment, the user would seamlessly switch from one hardware device to another and continue working without experiencing loss of functionality from one device to another. A company allowing a user to access data from personal mobile devices, is thus exposed to the risk of company data being synchronised to external applications and servers incremental to the risk of company data being stored on mobile devices which are susceptible to theft or misplacement.

Research have been conducted on the mobility and BYOD trends, but the incremental risks related to the synchronisation of data into one liquid platform uploading and downloading from all connected networks have not been researched. Liquid computing necessitates an understanding and response to these incremental risks and the mitigating controls needs to be clearly defined.

1.3 Research Objective

Past approaches to mobility give little attention to the problems regarding disconnection, hibernation and reconnection outside the file system context (Snoeren, Balakrishan & Kaashoek, 2001). Mikkonen and Systä (2014: 338–343) argued that the need to synchronise and back up data between different devices is still a major hassle, as is the requirement to manually define e-mail accounts, bookmarks and preferences. Automatic synchronisation removes the hassle from the user, but is currently only limited to devices and applications operating on the same platform and communicating with the same protocols (Mikkonen & Systä, 2014: 338–343).

Previous studies have already identified that liquid software eliminates the protection provided by the machine-specific restrictions that secure the data on that machine (Mikkonen & Systä, 2014: 338–343). Management of entities utilising liquid computing needs to be aware of the risks associated with the technology and implement sufficient controls to mitigate these risks (IT Governance Institute (ITGI), 2003: 26).

The objective of this study is to identify the incremental risks associated with autonomous synchronisation and recommend controls to mitigate these risks. This study quantifies the identified risks and controls in order to evaluate whether the recommended controls mitigate the identified risks to an acceptable level.

1.4 Research methodology

The research is a non-empirical, qualitative study. The study was performed using the following steps to address the research problem:

Step 1: Performed an extensive literature review of popular press articles, electronic sources, white papers, theses, books and accredited articles in local and international journals on the technologies enabling liquid computing.

Step 2: Based on the underlying technologies that enable liquid computing, this study provides a definition of liquid computing. The definition was used to identify what constitutes liquid computing and which enabling technologies are imperative to a liquid computing environment. This definition assisted in identifying relevant literature for the literature study.

Step 3: Based on the knowledge acquired in the literature review, the risks incremental to liquid computing was identified. These risks were quantified based on the likelihood to occur as well as the severity of the impact on the business in the event that the risk does occur.

Step 4: The identified risks were mapped to the different processes of the Control Objectives for Information and Related Technology Version 5 (COBIT 5) framework. The framework was used to identify possible risks that might not have been identified based on the literature review.

Step 5: Mitigating controls were recommended for each risk identified, based on the Control Objectives for Information and Related Technology. The mitigating controls proposed were quantified based on their success rate in notifying management of the risk and the ability to contain the consequences in the event that a risk did occur.

Step 6: The unmitigated risk remaining, after implementing the recommended controls for each risk, was calculated.

1.5 Key terms and concepts

The following list contains certain key terms used throughout this study. This list does not attempt to provide formal definitions, but provides context on how the terms should be interpreted for the purposes of this study:

Accidental espionage:	Unintentionally seeing or overhearing confidential information.
Cloud computing:	Utilising servers and software not owned by the users through an internet connection.
Data:	Raw, unprocessed facts, databases, information and digital files.
Incremental risk:	An existing risk that is amplified as a direct result of a specific event / chain of events.
Interoperability:	Seamless collaboration of hardware and software regardless of the device or software manufacturer.
IT Gap:	Misalignment between business goals and IT solutions designed to achieve these goals.
IT Alignment:	Designing and implementing IT solutions which fit into the operational strategy of a business and aids the enterprise in achieving its business goals.
IT environment:	Hardware, software, connections, networks, servers, human resources and business partners involved in the digital storage, processing and retrieval of information of an enterprise.
Liquid computing:	A scalable state of computing where all devices are constantly updated with data from the datacentre and the computing experience is seamlessly handed off between devices connected to the network.
Malware:	Malicious software that attacks electronic devices and data.
Millenial:	Person born during the 1980's or later.
Mobility:	Connecting mobile devices to computer networks.

Seamless mobility:	Seamless handoff of tasks between computers and different mobile devices.
Synchronisation:	The process of copying data and information on a network to all connected devices (often through an internet connection) and ensuring that all devices constantly contains updated information locally.
Unmitigated risk:	The risk remaining after controls were designed and implemented to mitigate risk.
Web 3.0:	Third generation data-rich web experience were machines interpret, share and act on data.

1.6 Layout and structure

The rest of the study is structured as follows:

- **Chapter 2:** A literature review was conducted in order to identify the components in a liquid computing environment. Once all these components were identified and understood, the characteristics present in a liquid computing environment were discussed and a definition for liquid computing was formulated.
- **Chapter 3:** An appropriate control framework was investigated and used in order to follow a structured approach to identify the risks incremental to liquid computing. These risks are discussed, mapped to the control framework and quantified in this chapter.
- **Chapter 4:** This chapter suggests controls to mitigate the risks identified in the previous chapter. The strength of each control is quantified based on the ability of the control to highlight the risk and limiting the impact of the risk in the event of occurrence.
- **Chapter 5:** The suggested controls are mapped to the risks and the unmitigated risk that remains after implementing the control, is quantified. Suggestions for further research are proposed.

1.7 Delimitations of the overall study

The study only focus on risks incremental to liquid computing. The study does not attempt to provide an exhaustive list of all risks and the focus is not on identifying risks associated with the underlying technologies enabling liquid computing. It is also not the purpose of this study to provide technical discussions on the technologies underlying a liquid computing environment.

The proposed control matrix only contains controls recommended to mitigate the risks incremental to liquid computing and it is not the aim of the study to propose an all-inclusive control matrix for enterprises utilising mobile technologies.

Chapter 2 – Defining Liquid Computing

2.1 Introduction and background

The new mobility culture surrounding how we work and use technology and the convergence of technologies has led to a new era in the IT evolution. This is an era where the digital profile is attached to the user and not the computing device used by the user. A user is now able to start a task on one device and continue with the same task on another. Similarly, internet search history of a user on a mobile device, will influence the ads and search results of that user when using another device. This era is liquid computing.

An investigation into the incremental risks of liquid computing requires a definition of the technology. In order to define the technology, the underlying technologies of liquid computing must be fully understood. The IT environment is constantly changing and liquid computing is an evolution of a number of enabling technologies. Once these technologies are identified and understood, the term liquid computing can be defined based on the common characteristics and technologies that enable it. A thorough understanding of these technologies is also necessary to fully understand the risks associated with liquid computing. Controls can then be suggested for the risks by using a structured approach of mapping the risks to the areas of an existing control framework.

Mikkonen and Systä (2014) argues that technological products undergo evolution during their lifecycles necessitating interoperability and adaptability to different needs in order to remain popular. Liquid computing is not a technology in its own right, it can be better explained as a natural evolution stemming from the use of different technologies in conjunction with each other. Mobility, BYOD and cloud computing all culminate into liquid computing.

Liquid computing can thus be described as a state of computing where processing, storage and data retrieval is not attached to a specific device or location, but rather to the user or user group. The less disruptive the state change between different computing devices, the more liquid the computing state (Satyanarayanan, Kozuch, Helfrich & O'Hallaron, 2005: 159).

In order to understand a liquid computing environment and the different stages of liquidity in computing, it is necessary to identify the components necessary for the operation of a liquid computing environment. These components on their own, do not constitute liquid computing, but liquid computing can only exist when all of these technologies are utilised together. The different components, which will all be discussed in detail in the following section, are:

- Hardware and software components, and
- Enabling technologies consisting of:
  - Mobility,
  - BYOD,
  - Cloud computing, and
  - Synchronisation.

2.2 Hardware components

Satyanarayanan *et al.* (2005) argues that the pervasive deployment of commodity hardware will liberate users from carrying a predetermined device, since seamless mobility will enable users to use any computing device to continue working on a project. This type of mobility or liquidity in computing requires common access to the data, regardless of the device being used. The following hardware components are an integral part of a liquid computing environment:

2.2.1 Mobile computing devices

These are any devices that can be used to connect to the database either to retrieve information or to edit/process information. In a truly liquid environment, the user interface and experience between different mobile computing devices should have only minor to no differences. This is being referred to as experience roaming or continuity (Wikman, 2015: 1). The processing capability and –speed of the hardware device would also have an impact on the degree of liquidity as the switch from a personal computer with high processing capacity to a cell phone or tablet with lower processing power should not negatively impact on the user experience in a liquid environment (Zhang & Adipat, 2005: 295).

2.2.2 Switches

Cisco (n.d.) explains switches as devices that connect networks and serve as controllers that enable devices in a network to talk to each other. In Gartner's IT Glossary, a switch is defined as: "A device that makes, breaks or changes connections in an electrical circuit; to shift to another electrical circuit by means of a switch" (Gartner, 2016). For a liquid computing environment to exist, connectivity between devices are of paramount importance.

2.2.3 Routers

Routers are devices connecting computing devices to the internet (Cisco, n.d.). Routers are responsible for routing the transfer of data through a network. The router is the device sharing the internet connection to multiple devices and it is responsible for hosting a network (Hoffman, 2015). Routers are necessary in a liquid computing environment to direct the transfer of data between the datacentre and the various devices connecting to the data for retrieval, upload, storage and/or manipulation of data.

2.2.4 Modems

The modem is the device responsible for connecting the router to the internet as it converts whatever internet structure the internet service provider supplies

(cable, telephone, satellite or fibre) into a standard ethernet output that can be connected to the internet (Hoffman, 2015). Many modern routers have built-in modems, but it is important to realise that it represents two separate hardware components that are necessary for a working internet connection – an imperative component in liquid computing.

2.2.5 Servers

A server is a computing appliance that creates, manipulates or provides information to other network-connected computing devices, using an application context (Gartner, 2016). Since liquid computing relies on mobility to be seamless between devices, the information or data should be common to all devices with access authorisation to the database. File servers centrally host data and make it available to computing machines and thus a server is an imperative component in a liquid computing environment (Christensen, 1997: 11). In this context, the server can refer to a cloud server providing access to data/information stored in the cloud or it could refer to an organisation server to which mobile devices have access through a virtual private network on the internet.

2.2.6 Connection mechanisms

This refers to whichever lines are used to connect different access points in the network. Mobile devices and desktop computers are connectable by many different connection mechanisms (Ulrich, Discolo & Alam, 2000: 10). Depending on the specific setup, this might be telephone lines connecting devices through a DSL service, it might refer to WiFi signals travelling between mobile devices and routers and it can also refer to mobile signals travelling between cell phone towers to transfer data packets (Goralski, 2009). As liquid computing refers to seamless switching between various devices, connection is a very important aspect of liquid computing and various connection lines may be used to establish connections between various devices.

2.3 Software components

Several software components will be necessary for a computer environment to be liquid. The following software components will be present in a liquid computing environment.

2.3.1 Applications

Considerations that had to be taken into account when making the internet accessible on mobile devices were: small screens, navigation, site structure and input methods (Buchanan *et al.*, 2001). Sarker and Wells found that ease of use and logical interface are more important to the user than the physical limitations of the device (Sarker & Wells, 2003: 35–40). An easy-to-use interface is critical to the successful adoption and use of applications (Zhang & Adipat, 2005: 293–308). Mobile applications are developed specifically for small mobile devices and they include news alert services, advertising, web portals and mobile commerce applications (Zhang & Adipat, 2005: 293–308). Satyanarayanan *et al.* describes personal productivity applications as the most valuable part of an ecosystem consisting of operating systems, graphical user interfaces, applications, user expectations and computing practices (Satyanarayanan *et al.*, 2005: 158). They continue to argue that skill in using the dominant application suite for a specific niche is essential for professional success (Satyanarayanan *et al.*, 2005: 159). Different applications are developed for different hardware devices and for the environment to operate in a state of liquidity, it is important that the various mobile applications mimic the layout and design of each other and the desktop applications. The more similar in architecture and interface the different applications are, the more seamless the transition will be for the user from one device to another (Mikkonen & Systä, 2014: 339). Another aspect of applications in a liquid computing environment is the applications installed on various servers in the environment, managing the synchronisation and updating of data to ensure that the central database is up to date with the latest changes and that the information from that database gets distributed and synchronised back to the devices with access to the network. Thus, the flow of data into and out of the database has to be managed by application software.

2.3.2 Operating systems

Operating systems are software that manage a computing device's resources and control the flow of information into and from the main processor thus providing the foundation on which applications, middleware and other infrastructure components function (Gartner, 2016). Popular desktop operating systems include Windows, MacOS and Linux whilst iOS and Android are the most used mobile operating systems. Since operating systems provide the user interfaces between the user and computer, they have a big impact on the perceived seamlessness of transitioning from one device to another. Applications developed for iOS might have a look and feel identical to the MacOS version as both of these operating systems are developed by Apple Inc. The Android version of the same application might have a completely different user interface, thus requiring adjustment from the user to switch between various devices. This user-adjustment impacts negatively on the computer liquidity as the transition from one device to another in a truly liquid computer environment should be seamless.

2.3.3 Firewalls

Firewalls screen network traffic and can keep unwanted traffic out of a private network and prevent intrusion (Gartner, 2016). Entire computers can be set up as firewalls, but since it is the software that is responsible for filtering the network traffic, it is categorised under the software components of a liquid computing environment. Firewalls are critical for local networks that connects to the internet (Gartner, 2016). Since internet connection is an imperative component of liquid computing, firewalls are equally important to keep the local network secure. Firewalls can also limit authorised users within a network to certain files or functions within that network. Specific users might be granted access to view data, but not edit it, while other users may be given access to edit and view data whilst being prevented from changing master file data. These access rights can be controlled by firewalls. The various stages of firewalls that a user has to move through to perform a specific task, will have a direct impact on the user's perception of speed and fluidity of the application and thus will influence computing liquidity. When accessing data on the local network from

an employer-provided workstation on site, the user might not have to pass through firewalls; whilst the user has to pass through various firewalls when connecting his personal tablet to his WiFi network at home and trying to access company data. This will result in perceived loss of speed at home which will impact negatively on the seamlessness or state of liquidity.

2.4 Enabling technologies

In section 2.1, it was explained that liquid computing is the collaboration of different enabling technologies into a new user culture where the computing experience is not attached to the specific device, but to the user profile. These enabling technologies will now each be discussed in further detail.

2.4.1 Mobility

The mobility technology refers to connecting mobile devices to the internet without the need of a cabled connection to the device. The popularity of mobility can be traced to the ability to deliver information to users when needed (Lee, Kim, Kim, Choi, 2002: 133–137). The rapidly expanding usage of networked-connected devices can be divided into the following different categories (Mikkonen & Systä, 2014: 338–343):

- Computers,
- Tablets and E-readers,
- Smartphones,
- Televisions and Game consoles,
- Car displays, and
- Gadgets and Wearables

With the exception of computers, all of these devices are enabled by the ability to receive mobile internet connectivity. Sarker and Wells state that the ability of wireless technology to enable mobile communication, mobile collaboration and mobile commerce can be described as its best selling points (Sarker & Wells, 2003: 35–40).

In 2007, Kim, Chan and Gupta had already found that mobile internet usage has surpassed stationary internet usage (Kim, Chan & Gupta, 2007: 111–126). A study conducted in the United States of America found that, by 2009 already, 63% of adult internet users accessed the internet using multiple devices with 54% of adult internet users accessing the internet wirelessly and 35% of adults reporting that they use cell phones to access the internet (Lenhart, Purcell, Smith & Zickuhr, 2010: 1–51). In the first half of 2015, 51% of all internet usage have been recorded from mobile devices (Chaffey, 2015). Smith found that smartphone ownership increased from 35% of all American adults in 2011 to 56% of American adults in 2013 while those indicating that they own any other cell phone decreased from 48% to 35% in the same time (Smith, 2013: 2). Smartphones have an increased ability to access the internet compared to conventional cell phones. Mobile devices delivers new services to existing customers as well as attract new customers (Kim *et al.*, 2007). Drawbridge, a company specialising in matching internet users across devices, has linked 1.2 billion users across 3.6 billion devices – up from 1.5 billion devices a year earlier (Tanner, 2015). This is an indication of the current growth rate of the mobility trend. Mobile application and services will continue to expand as phone networks evolve into fourth-generation (4G) and mobile devices become more common and inexpensive (Aker & Mbiti, 2010: 1).

Reliable communication of information is imperative in a mobile environment. Banerjee, Wu & Das defines mobility as follows: “Mobility means the ability of a mobile host to overcome the location-dependent nature of IP addresses by a suitable translation mechanism and to send and receive datagrams efficiently from any location” (Banerjee, Wu & Das, 2003: 54). Communication is enabled by protocols. Passerone, Rowson & Sangiovanni-Vincentelli defines a protocol as: “the legal sequences of values that may appear on the ports from the onset to the end of the data transfer” (Passerone, Rowson & Sangiovanni-Vincentelli, 1998: 9). A protocol typically consists of a set of atomic operations (Narayan & Gajski, 1995):

- waiting for an event on an input control line,
- assigning a value to an output control line,

- reading a value from input data lines,
- assigning a value to an output data line, and
- waiting for a fixed time interval.

Liquid computing relies on wireless connections and communication of data often in the form of Wifi technology. Wifi technology uses radio waves to provide network connectivity (CCM, 2016). Some of the central issues in wireless communication include how the device connects to the network, how mobility is supported as the device moves from cell to cell between networks and how multiple users are accommodated (Ayyash, Elgala, Khreishah, Jungnickel, Little, *et al.*, 2016: 66). When two devices use different signalling conventions, synthesising the interfaces between the communicating devices becomes problematic (Passerone *et al.*, 1998: 8). When two devices use compatible protocols, communication is possible as soon as the communication ports are connected, however, when incompatible protocols are being used between the two devices, an interface process needs to be inserted between the two components to enable communication (Narayan & Gajski, 1995). Narayan & Gajski explains that an interface process will respond appropriately to the control signals of the two incompatible protocols and transfer the data between them, or in layman's terms, translate the one protocol into the other (Narayan & Gajski, 1995). Protocol interface is thus imperative to the communication of information between various devices using different protocols.

2.4.2 Bring-Your-Own-Device (BYOD)

Bring your own device (BYOD) is an inevitable IT evolution because it comes from the convergence between cloud and mobility technologies (Scarfo, 2012: 447). This is a trend where staff are allowed to bring their personal mobile devices like smart-phones, tablets and laptops to work to access databases and applications owned by the employer (Singh & Phil, 2012: 1). This trend increases the flexibility and availability in worklife of employees and thus it is demanded by employees that organisations adopt a BYOD policy (Singh & Phil, 2012: 1). It is argued by Self that BYOD strategies are usually driven by consumer preference rather than corporate initiative and that there is potential

benefit for both parties since it increases mobility, flexibility and employee satisfaction which increases productivity (Self, 2013: 19).

The alternative to BYOD is a policy of use-what-you-are-told (UWYT). This is a culture where the employer provides company owned devices and employees can only access company resources from these devices (Singh & Phil, 2012: 2). In a UWYT policy, the employer has to bear the initial capital outlay of the hardware as well as the software licenses and maintenance of the whole infrastructure which includes, but is not limited to, the hardware devices used by employees.

One of the biggest financial benefits of a BYOD policy is that the costs of electronic devices are shifted from the organisation to the employees. This reduces cost while maintaining employee satisfaction (Comisky & Diamond, 2014: 386). When organisations need to supply electronic devices, they may be slow to adopt to new technology as the cost of hardware is a big expense and technology is ever changing resulting in hardware becoming obsolete on a regular basis (Imazeki, 2014: 240). There is also the risk of employee abuse of company-supplied hardware in a UWYT environment. If a company adopts a BYOD policy, it transfers these costs to the employees which makes innovation more affordable to organisations (Imazeki, 2014: 240). Initial and maintenance cost of devices rest on the employees of companies where a BYOD policy is deployed (Kabanda & Brown, 2014: 1).

Another advantage of a BYOD policy is that the organisation is not liable for pirated software on the device as the device is not the property or under the control of the organization (Kabanda & Brown, 2014: 1). The cost advantages of a BYOD policy renders this especially useful for small and medium-sized enterprises that cannot necessarily afford to invest in electronic devices that are prone to redundancy.

Cost advantage is not the only reason for entities electing to adopt this policy. Scarfo argues that employees utilize their own devices more effectively and that a BYOD policy opens up more opportunities to collaborate which results in increased productivity, especially for activities where mobility is of importance (Scarfo, 2012: 446). Singh and Phil argues that one example of higher productivity is the reduced training time when employees use their own devices with which they are already familiar (Singh & Phil, 2012: 4). Singh and Phil studied employees from different sectors and found that 45.5% of respondents said that increased mobility is the most important factor of a BYOD strategy, while 40.9% felt improved efficiency and productivity was the most important advantage (Singh & Phil, 2012: 8). A BYOD strategy does not only increase employee efficiency, but it also extends beyond office hours as employees use their personal devices to communicate with co-workers, customers and suppliers and thus they can communicate from anywhere (Comisky & Diamond, 2014: 386). Singh and Phil echoes this stance in their argument that BYOD policies enable a company to get higher return on employee time (Singh & Phil, 2012: 10).

2.4.3 Cloud computing

Gartner's IT glossary defines cloud computing as "a style of computing in which scalable and elastic IT-enabled capabilities are delivered as a service using Internet technologies" (Gartner, 2016). Cloud computing refers to applications delivered as services over the Internet as well as the hardware and software that provide those services (Armbrust, Fox, Griffith, Joseph, Katz, Konwinski, Lee, Patterson, Rabkin, Stoica & Zaharia, 2009: 7–13). Buyya, Yeo, Venugopal, Broberg and Brandic proposed the following definition for cloud computing: "A Cloud is a type of parallel and distributed system consisting of a collection of inter-connected and virtualized computers that are dynamically provisioned and presented as one or more unified computing resource(s) based on service-level agreements established through negotiation between the service provider and consumers" (Buyya, Yeo, Venugopal, Broberg & Brandic, 2009: 3)

Cloud computing enables providers of the technology to build large data centres at low cost and sells computing as a utility (Basson, 2014: 1–67). Users of this trend are attracted by lower costs of utilising cloud computing as opposed to developing or buying “in-house” software (Buyya *et al.*, 2009: 1–17). According to Armbrust *et al.* cloud computing not only refers to the applications delivered as services over the internet, but also the hardware and systems software in the datacentres that delivers these services (Armbrust *et al.*, 2009: 7).

Cloud computing has led to the proliferation of Software as a service (SaaS). SaaS separates ownership of software from its use by delivering the software to the user device over an internet connection while the software is housed on a server, often hosted in the cloud (Turner, Budgen & Brereton, 2003: 38). This culture attaches the computing ability to the user profile as opposed to the conventional model where the ability of processing the data is attached to the machine or device with the relevant software. As long as the user has access to a working internet connection, the user can log in with a username and password and continue processing, regardless of the device.

2.4.4 Synchronisation

Synchronisation is defined as: “the establishment of common timing between sending and receiving equipment” (Gartner, 2016). Filemaker, a subsidiary company of Apple, describes synchronisation as keeping two or more databases up to date with each other’s data changes (FileMaker, 2010). Since liquid computing involves handing off tasks seamlessly between different devices, constantly synchronising data across the various devices is imperative to a liquid computing environment. Processing requests from the mobile device should synchronise and update to the datacentre in order to ensure reliable and timeous information are housed in the datacentre. Datacentre updates should push synchronisation to all connected devices as and when changes to the data are requested.

2.5 Characteristics of Liquid Computing

Section 2.2 and 2.3 provided a brief discussion on the hardware and software components present in a liquid computing. Section 2.4 then discussed the different technologies which, in combination with each other, culminates in liquid computing. Given the components necessary to enable a liquid computing environment, the following characteristics are typically present in an environment of liquid computing. This section will briefly explain the most common characteristics of a liquid computing environment.

2.5.1 Scalability

In a liquid computing environment, the number of devices connected to the environment is ever-changing. Users can connect multiple devices and the number of users is also unlimited. The size of the network can be constantly increased by adding more devices.

2.5.2 Centralised data

The data has to be centralised and all devices should update to this central data. This data should also synchronise back to all connected devices. This ensures that all the information on all devices are up to date.

2.5.3 Synchronisation

The computing experience will only be liquid if changes to data are synchronised to all devices. Synchronisation failure will result in obsolete data on devices which will result in users making uninformed decisions. Synchronisation will also ensure that the transition from one device to another will be seamless for a specific user, as the user will be able to continue tasks on a second device exactly where he left it off on a first device.

2.5.4 Conflict management

Although this characteristic might be regarded as part of synchronisation, it is imperative to successful liquid computing and thus discussed separately. Replication between various devices and centralised data might result in

conflicts as users might edit on the same dataset (Wikman, 2015). It is important that these replication conflicts are managed to ensure that the integrity of the data is protected at all times.

2.5.5 Connectivity

Internet connectivity is an imperative characteristic in a liquid computing experience. Without connectivity between a mobile hardware device and the centralised database, no synchronisation can occur which will result in uninformed decision making and obsolete information. This might also result in counter-productivity between various users as users might duplicate tasks.

These are the minimum characteristics that will be present in a liquid computing environment. Depending on the level of liquidity required, several additional characteristics will present itself. Liquid computing can therefore be defined as a scalable state of computing where all devices are constantly updated with data from the datacentre and the computing experience is seamlessly handed off between devices connected to the network.

2.6 Conclusion

Liquid computing is not a technology. Liquid computing is better described as a behaviour driven by the use of multiple enabling technologies. Wikman argues that the ability to move fluidly from one device to another is a central aspect of a true, multi-device computing experience (Wikman, 2015: 1). This fluidity in computing where the computing task at hand can be seamlessly handed off from one hardware device to another, regardless of location or user, is referred to as liquid computing.

Figure 1 below represents how the enabling technologies (as explained earlier in this chapter), collaborates to form a liquid computing environment.

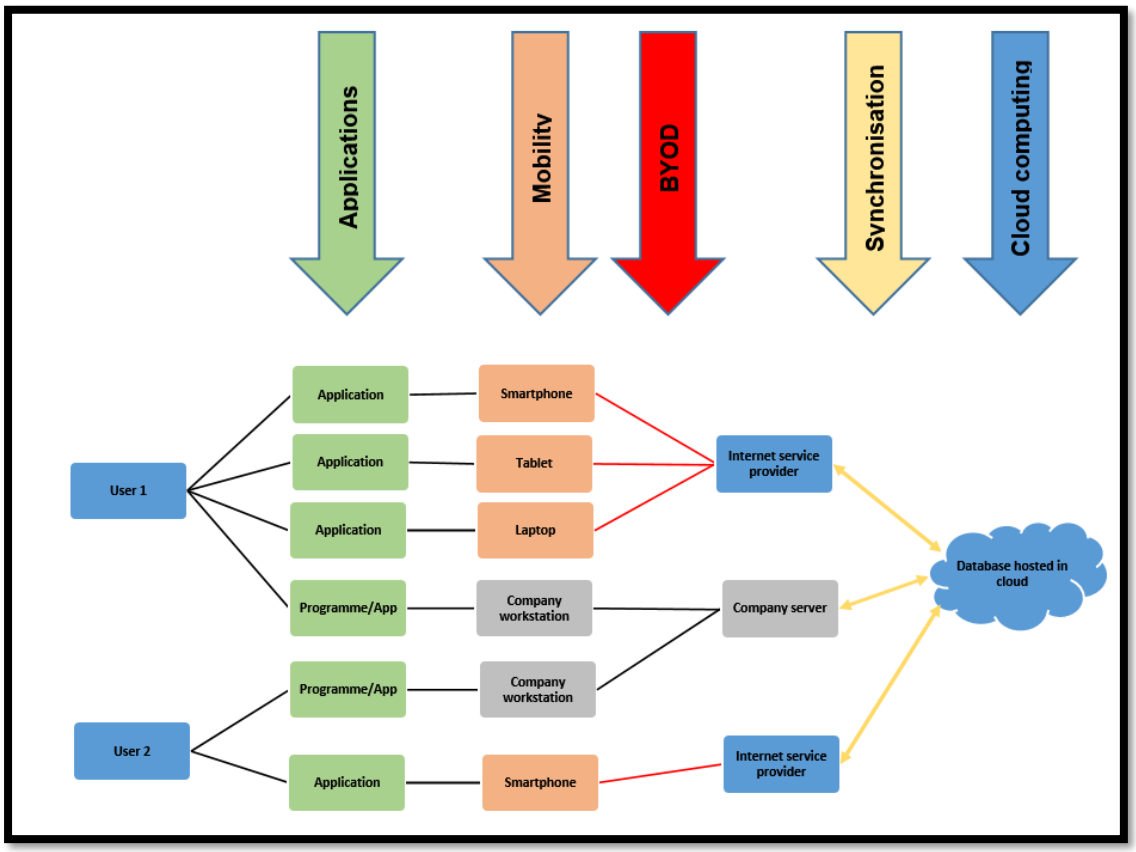

Figure 1 Overview of liquid computing

(Source: Author's own)

From Figure 1 it can be seen that User 1 may start on a project on his desktop at work and continue working seamlessly on the same data from his smartphone, tablet or laptop anywhere else, whilst User 2 might be working on the same project from another location on his smartphone. This liquid state of computing is enabled by the data being hosted in the cloud, allowing the applications on the company server and various mobile devices to access the data by means of a BYOD strategy. Synchronisation of all of these applications and devices to the central database, ensures that the central database remains up to date with the newest information and that computing remains fluid between different devices and users.

According to Satyanarayanan *et al.*, seamlessly transitioning without distracting the user, is an important attribute of mobile computing (Satyanarayanan *et al.*, 2005: 159). They continue to argue that human attention is a consumable resource that is consumed by needs such as adjusting to an unfamiliar physical environment and it is thus made even scarcer by the demands of mobility (Satyanarayanan *et al.*, 2005: 160). Seamlessly switching between different mobile devices thus increases productivity and therefore the argument can be made that the more liquid a computing environment, the more productive the users in said environment can be.

Various different stages of liquid computing can exist. A computing environment is only truly liquid when the user experience in interface, speed and capability is unaffected by the device used, or location of the user, with continuous synchronisations between devices running autonomously.

Increased liquidity will result in more risks being present which will consequently necessitate more controls. The degree of controls in a specific environment will dictate additional characteristics. Since risks and controls are dependent on the specific setup, the characteristics specific to the risks and control environment are not included in this chapter. The characteristics described in this chapter are only those generic to establishing a liquid environment and the incremental characteristics to establish a well-controlled liquid computing environment will be discussed in the chapter dealing with controls.

The following chapter investigates the risks that are incremental to a liquid computing environment.

Chapter 3 – Risks incremental to Liquid computing

3.1 Background

Spremic defines an IT risk as the likelihood that a threat-source can negatively impact information systems assets, information systems services and technology and key business processes or the entire organisation (Spremic, 2012: 299). Risk assessment is the process of identifying these potential threats (Azizi & Hashim, 2010: 333). It (risk assessment) involves scoring alternatives based on their likelihood to result in deviations from the expected return (Iyer & Bonissone, 2007: 272). Fast changing technological environments introduce additional risk since it creates opportunities and consequently facilitates threats (Orman, 2013: 23). In order to assess these risks properly, Toth (1994: 22) argues that expert knowledge is required. The Sarbanes-Oxley Act of 2002 prescribes that public companies should utilise a risk control framework in the assessment of risks (Friedhoff & Mansouri, 2016: 1).

This chapter will first discuss governance and IT governance. The IT gap and alignment will then briefly be explained after which a brief discussion of possible frameworks will follow, that might be used in the assessment of risks specific to liquid computing. An appropriate framework will then be selected, which will then be used to assess risks incremental to liquid computing.

3.2 Governance

Since liquid computing facilitates threats, organisations need to have policies and procedures to govern this technology as a strategic asset. Sahd points out that those charged with governance should specifically tailor the governance system of an organisation for IT assets in order to ensure alignment with business strategies (Sahd, 2015: 13).

3.2.1 Corporate Governance

Corporate governance is defined as “procedures and processes according to which an organisation is directed and controlled” and it (corporate governance) includes activities of the Board and relationships with stakeholders (Krechovská & Procházková, 2014: 1145). The Board should be responsible for the governance of an enterprise’s risk and refrain from risk management becoming detached from the company’s business (IODSA, 2009). The Third King Report on corporate governance goes further to state that risk management should be an ongoing process and should be performed on all levels of an organisation (Institute of Directors Southern Africa (IODSA), 2009). This includes the management of strategic and operational risks.

Strategic objectives can only be obtained if corporate governance in an organisation is sound. Corporate governance is based on the agency theory as it deals with the separation of duties between principals and managers (Grose, Theodoros & Chouliaras, 2014: 371). Good governance increases a firm’s market valuation, provided that it increases returns to the shareholders and that the stock market is sufficiently efficient to ensure that share prices reflect fundamental values (Bai, Liu, Lu, Song & Zhang, 2004: 601). Returns of shareholders are increased not only by directly increasing revenue but also by limiting losses. Management of risk is therefore imperative to increasing shareholder returns. Risk management is also an important aspect in ensuring going concern.

The governance practices of a company should aid a company in securing it as a going concern (Krechovská & Procházková, 2014: 1145). This implies that a company keeps track with changing externalities such as technology. A company should thus be able to adjust governing practices to suit the changing environment in which said company operates (Sahd, 2015: 13). The emergence of liquid computing as a resource should therefore be managed as part of a company’s corporate governance on an ongoing basis.

3.2.2 IT Governance

Symons (2005: 2) defines IT governance as the process by which decisions are made around IT investments. IT governance is a subset of corporate governance (Webb, Pollard & Ridley, 2006: 3). Sahd (2015: 14)argues that IT governance is achieved through leadership and structures within an organisation as well as a framework that encourages desirable behaviour in order to direct, manage, control and maintain IT investments and the application and use of IT. Bradley and Pratt (2011: 2) defines IT governance as the capacity of top management to control the formulation and implementation of IT strategy by means of organisational structures and processes that will ensure that the IT initiatives of an enterprise sustains and extends the strategy and objectives of the organisation. Governance of IT should not only address the organisation's investment in IT but also the operational use of IT in the organisation (Sahd, 2015: 14, 2016: 291). Gartner's IT Glossary identifies IT-demand side governance as well as IT-supply side governance. In terms of the glossary, demand side governance of IT refers to evaluation, selection, prioritisation and financial support of investments in IT as well as administration and management of its implementation and realisation of benefits from this investment while supply side governance refers to the IT function being used effectively, efficiently and appropriately and that it complies with relevant regulations and policies (Gartner, 2016).

Webb, Pollard and Ridley (2006: 4) explains the relationship between objectives of Corporate governance and those of IT governance at the hand of the following table:

Table 1 Comparison between Corporate governance and IT governance

Corporate Governance	IT Governance
Strategic direction	Strategic alignment
Delivery of business value	Delivery of business value through IT; exploiting opportunities and maximising benefits
Performance management	Performance management; IT resources must be used responsibly
Risk management	Risk management; IT related risks to be managed appropriately
Policies and procedures	Policies and procedures
Control and accountability	Control and accountability

(Source: Webb *et al.*, 2006: 4)

Companies with IT governance strategies stand a much better chance of managing risks when compared to companies without such strategies (Bradley & Pratt, 2011: 3–4). This theory is enforced by Web, Pollard and Ridley who argues that IT governance directly influences the benefits generated by organisational IT investments (2006: 1). These benefits can only be derived if there is alignment between strategic objectives and IT governance objectives.

Bruwer lists advantages of, and risks to, implementing and non-compliance with IT governance principles, respectively, which have been summarised in the table below:

Table 2 Advantages and disadvantages of IT governance principles

Advantages to implementing IT governance principles	Risks of non-compliance with IT governance principles
Strategic alignment between IT and business goals that will create a competitive advantage	Operational risks
Increased risk management and improved decision making	Confidentiality, reliability and authenticity of data under threat
Compliance with laws and regulations	Unauthorised access and changes to IT system which could lead to unavailability and impaired functionality

(Source: Bruwer, 2013: 24)

3.2.3 IT Gap and alignment

The IT governance process is often ad hoc and informal without mechanisms to measure and monitor the outcomes of decisions (Symons, 2005: 2). This ad hoc management of IT, results in the IT gap. Rudman (2010: 3253) describes the IT gap as a problem that arises as a result of management not understanding control techniques and technology used whereas the IT professionals neither understands the control model nor the control frameworks.

Rudman (2010: 3254) states that management develops policies, based on a framework, with specific objectives in mind and then derives processes to implement these policies whilst the IT department, who is responsible for the operation and maintenance of the technology and controls, acquires technology and builds and configures controls on an ad hoc basis without conceptualising the controls in terms of management's objectives. This results in the actual controls implemented being far removed from the board's expectation in terms

of IT governance (Sahd, 2015: 16). Rudman (2010: 3254) suggests that a control framework should be used to assist in developing appropriate IT governance that links information technology and resources to the business requirements.

3.3 Control frameworks

Security risks can be mitigated by implementing internal controls at different levels (Rudman, 2010: 3253). Control frameworks are defined by Webb, Pollard and Ridley (2006: 4) as any set of processes, procedures and policies that enable an organisation to measure, monitor and evaluate their situation in relation to predefined factors, criteria or benchmarks.

Rudman (2010: 3253) argues that Control Objectives for Information and related Technology (COBIT) has been successful at a high level in addressing security risks posed by unauthorised entry. COBIT is generally used as a benchmark framework and is often used for audits (Sahd, 2015: 18). COBIT allows management to bridge the gap between control requirements, technical issues and business risks and enables policy development (Susanto, Almunawar & Tuan, 2011: 27). Other frameworks that are often used in IT governance, are the IT Information Library (ITIL) and ISO/IEC 27000 series (Sahd, 2015: 18). According to Sahd (2015: 18), ITIL is used for describing and designing IT processes while ISO/IEC 27002 is used for security issues and mitigation of specified risks. Since this study deals with the incremental risks and controls of liquid computing, COBIT 5 and ISO/IEC 27000 series would be the most appropriate frameworks to evaluate the technology against. ISO/IEC 27001 has been developed to protect the information assets of businesses on a process-based approach (Fomin, De Vries & Barlette, 2016: 15). The scope of COBIT 5 is IT Governance whilst the scope of ISO 2700 series falls on information security (Susanto *et al.*, 2011: 27). COBIT 5 will thus be utilised to identify the risks and areas that should be addressed whilst the ISO 2700 series will assist in suggesting controls for the identified risks.

3.4 Risks of liquid computing

Risks associated with IT are often the same as risks to the business, since an increasing amount of organisation's value propositions are built on IT (Symons, 2005: 6). IT risk represents the likelihood that a given threat-source can exercise a potential vulnerability and negatively impacts the information system assets, services, technology, key business processes or the whole organisation (Spremic, 2012: 299–300). Orman (2013: 23) argues that technology is a source of risk, not only because it often had unintended consequences, but also because accelerating technological change creates compound risks resulting from multiple interacting technologies. While technologies are created to create new efficiencies, these immediate efficiencies introduce new uncertainty and risk (Orman, 2013: 23). Risk assessment allows for the identification of potential risks to a project and performing this assessment regularly will allow for continuous improvement in order to stay ahead of changing levels of risk (Azizi & Hashim, 2010: 333). During risk assessment, risks are usually assigned to different alternatives and it is common for these risk assignments to come from a predefined set of risk classes (Iyer & Bonissone, 2007: 272). Risks should be quantitatively determined and prioritised in order to produce a prioritised risk matrix during risk management (Toth, 1994: 179).

It is important that organisations have policies in place to deal with the challenges brought by new strategies (Singh & Phil, 2012: 11). Some of the challenges associated with mobile strategies are listed below (Scarfo, 2012: 448):

- Enforcing the security policies of the organisation on the mobile devices of the employees,
- Lost or stolen devices containing sensitive data or information belonging to the organisation,
- Sensitive data confidentiality and integrity protection when accessed or stored on a mobile device,
- Threat management on mobile devices
- Supporting new device types, and
- Creating security policies for mobile devices.

Scarfo argues that these challenges can be categorised into three different types of threats (Scarfo, 2012: 448):

- Access to data and applications,
- Attacks on the devices and the networks, and
- Data protection.

Cloud computing solves many problems, but it also brings its own set of challenges. The top 10 obstacles to cloud computing, as identified by Armbrust *et al.* are (Armbrust *et al.*, 2009: 9):

- Availability of service,
- Data lock-in,
- Data confidentiality and auditability,
- Data transfer bottlenecks,
- Performance unpredictability,
- Scalable storage,
- Bugs in large distributed systems,
- Scaling quickly,
- Reputation fate sharing, and
- Software licensing.

Most of the risks incremental to liquid computing relates to the privacy and integrity of data, since data will be constantly synchronised to and from personal devices of users utilising different hardware and operating systems. Risks will therefore be addressed in the following order:

- Risks pertaining to privacy of users and data,
- Risks pertaining to the integrity of data, and
- Other risks.

3.4.1 Risks pertaining to privacy of data

Liquid computing gives rise to several risks pertaining to the privacy of data. One successful breach of security on the IT of an enterprise, can result in

serious financial loss and reputational damage (Hardy, 2006: 55). Since synchronisation is autonomous in a truly liquid computing environment, the user might not even be aware that data is being copied, overwritten or synchronised. This might result in personal data of the user being synchronised to servers of third party service providers and employees. Autonomous synchronisation may also result in confidential company data being copied to unauthorised servers linked to the user's device.

3.4.1.1 Risks of loss of control over information

Comisky and Diamond (2014: 395) address the problem that trade secrets and client lists might be saved on personal devices of employees where an employer uses a BYOD strategy. Documents, spreadsheets and contact information might be saved on personal devices or automatically saved to personal devices when user profiles are linked to mobile devices to synchronise contacts, calendars and documents. If the user connects his device to a personal profile on another platform, such as Gmail account or Dropbox, the device will prompt the user whether access should be allowed to the information on the device. In order for the synchronisation and backup to succeed, the user will allow this which might inadvertently also synchronise unintended information. It is also important to note that synchronisation is a process of continuous updating and such information will constantly be kept up to date on all platforms linked to the device (Farrow, 2006: 2).

Scarfo (2012: 449) explains that the user will have to pass through all the security measures of the organisation on initial connection but once the user was successful in first access, he will be able to access the data again without passing through security. When continuous synchronisation is selected, such as the case in liquid computing, the access to the data is continuous and the device will be saving data from the employer's database constantly as well as upload it to any other server where the user has also connected a profile. As long as the user profiles are linked, the employer's information will thus be synchronised to external servers over which the employer has no control. This

increases the risk of data theft and effectively negates all data access controls the employer might have on its own servers.

3.4.1.2 Risk of device theft

In order to protect information system resources, they should be secured (Susanto *et al.*, 2011: 23). Access cards, keys, security guards and alarm systems are ordinarily used to protect the physical assets of organisations. These security measures also provide protection to the organisation's data. Logical access controls such as passwords and access control matrixes are not uncommon.

Data is downloaded or synchronised to personal user devices used to access company resources. The high cost of data and intermittent and slow internet connectivity in Sub-Saharan Africa have increased the need to download data to a local drive or device in order to improve processing efficiency and fluidity (Alfreds, 2016). This results in data being saved to mobile phones, tablets and laptops which are at much higher risk of theft due to the increased mobility that comes with these devices. COBIT 5 specifically states that physical protection of endpoint devices is an activity the enterprise should entertain (ISACA, 2012a: 159). The employer / enterprise has no control over the aloofness and security employed by the user with regards to his / her own personal devices (Samaras, Daskapan, Ahmad & Ray, 2014: 1). The security of data belonging to the enterprise is thus as vulnerable to unauthorised access as a mobile device is susceptible to theft.

3.4.1.3 Device disposal

DSS05.03 of COBIT 5 deals with the management of endpoint security (ISACA, 2012a: 159). Mobile devices in a liquid computing environment are the endpoints, since liquid computing allows for all data to be accessed and used on mobile devices. COBIT 5 specifically mentions that endpoint devices should be disposed of securely (ISACA, 2012a: 159). Mobile devices have limited lifespan. In South Africa, cellular telephones are seldom used for periods in excess of two years by one user; since it is common practice amongst mobile

service operators to provide two-year contracts that offer device renewals. The evolution of technology and advances in processing capabilities of devices result in tablets and cellular telephones becoming obsolete in short timeframes. These devices are often very costly to acquire. This high cost and fast evolution of mobile technology result in device trade-in, reselling of devices on a second-hand market or handoff to relatives or friends.

The enterprise utilising a BYOD strategy has no control over how an employee disposes of his mobile device. In a liquid computing environment, where data is constantly synchronised through all devices, sensitive data might be downloaded to an employee's personal device. Upon disposal of this device, it is important to delete all company data and to delink this device from any user profiles that might cause synchronisation in future. If a device is not unauthorised / delinked, deletion of company data from the device will have no avail, as the device will download all the deleted data upon the next synchronisation session.

3.4.1.4 Risk of unauthorised access of devices

Corporate data is being delivered to devices that are not managed by the organisation (Kabanda & Brown, 2014: 2). Protecting devices only against theft is not comprehensive physical protection of the endpoint device. During a device's lifecycle, it is exposed to various different situations, people and circumstances. The owner of the device will not be at a maximum level of alertness and awareness of security regarding his / her mobile device at all times.

The risk of unauthorised access to data on a device is not limited to the disposal or theft of a device (Scarfo, 2012: 448). Passwords are less likely to be enabled when devices are left temporarily unattended. The unlocked, unattended device is at risk of unauthorised access. This unauthorised access to information could be malicious and intentional or unintentional. Regardless of the intent, the organisation is put at risk by the behaviour of the employee. This risk is a direct

consequence of enterprise information being synchronised to the employee's device.

3.4.1.5 Accidental espionage

Liquid computing enables users to complete office tasks away from work. Time that would traditionally be unproductive, such as waiting in a doctor's waiting room, waiting at an airport or standing in a queue can now be used to complete unfinished work assignments. Self (2013: 48) argues that an inherent, consistent and tireless understanding and appreciation for the concept of information security, only exists in a perfect world. Employees are often unaware of their surroundings. This might expose sensitive information to unauthorised individuals. Logos and mastheads are instantly recognisable and would provide context to whomever sees the information. The enterprise is thus constantly at risk that employees might unintentionally allow unauthorised members of the public to see confidential information without the employee him- / herself realising that he / she is disclosing the information.

3.4.1.6 Accidental disclosure

Mobile devices have evolved from simple communication tools into service delivery platforms (Kabanda & Brown, 2014: 2).The invasion of personal devices by employer data through synchronisation poses the risk that users might accidentally send work related information to private contacts. Applications are developed for ease of use and immediate gratification (Scarfo, 2012: 447). Attaching files to messages and emails are seamless and instantaneous. A user might accidentally attach a confidential document to an instant chat or email to a personal contact, effectively disclosing the information to a person without authorisation. The risk of accidentally disclosing information in this way is not unique to liquid computing, but the merger of work and personal life in one device, increases the likelihood of this risk occurring.

3.4.1.7 Risk of interception of information during communication

Sahd (2016) explains that wireless networks were traditionally not built for ubiquitous mobility or the delivery of services to critical business operations. A

liquid computing environment is enabled by constant communication of data – often over wireless networks. Synchronisation of data is imperative to the computing experience being truly liquid. Various different networks and service providers could be participants in this communication. Sahd (2015: 54, 2016) also identified that mobile wireless networks are often more vulnerable to malicious attack and interception. Communication between the personal computers of the enterprise and its server would be in a secure network over which the enterprise has control. The enterprise can set up as many firewalls and protection as it deems necessary. Partitioning of drives with stringent access controls matrixes can limit employees of the company to data. When access is allowed to mobile devices, access controls and user profiles are still utilised to restrict authorised users to specific data.

The enterprise does not have control over the network or service provider utilised to synchronise data to user devices in a liquid environment. When synchronisation is done over mobile data, mobile telephone service providers provide the network infrastructure. The high cost of mobile data and limited data coverage in South Africa results in many users reverting to wireless networks in the form of WiFi. Smart devices are often set to only synchronise data-heavy applications over WiFi connections to limit the user's data cost. Most synchronisations will thus only take place over WiFi networks over which neither the user nor the enterprise will have control. WiFi hotspots are a common phenomenon in public areas and users often cease the opportunity of this "free internet" to update and synchronise applications. During these connections, the information often travels through unsecured communication channels, routers and servers and are at risk of being intercepted, copied or changed. An unsecured WiFi network might copy all information travelling through its routers and neither the enterprise nor the user would realise that information was stolen.

Another privacy risk resulting from liquid computing is that SaaS enables the user to use any device with internet connectivity to continue a particular task. The user's processing ability is not limited to devices authorised for use by the

organisation, but to any device that can connect to the internet provided the user enters valid user credentials (Armbrust *et al.*, 2009: 7). This control is insufficient for user validation since credential managers on computers can be set to remember passwords. The risk thus arises that a public device will remember the password and an unauthorised user would also be able to access the data on that same computer. This risk reveals itself in cases where public computers (such as in internet café's, airports, libraries, schools and universities) are used to log in to user profiles. A login in a public computer area to quickly complete an urgent request, might expose confidential information to numerous and prolonged instances of unauthorised access.

3.4.1.8 Loss of personal information of users

Bruwer and Rudman (2013: 42; 2015) identified the intrusion and capturing of sensitive information without authentication as one of the risks to Web 3.0. Synchronisation entails copying data from server to device and from device to server. Personal data from user's devices can unintentionally be copied to servers. Users use usernames and passwords to access user profiles on servers in order to use personal mobile devices as extensions of office computers. Applications are developed for ease of use and seamless transitioning between devices (Scarfo, 2012: 447). An application may be used for personal and professional purposes. Once a user authorises and application to initiate synchronisation by entering a username and password and authorising a device, personal data of the user will be copied from the device to the database.

Dropbox is an example of such an application that is commonly used to store personal data and also used in the professional environment. A user might access his or her dropbox account from a work computer to backup files in order to later access the files from home. All personal data contained in that user profile's Dropbox account will synchronise to all devices signed in to the account. Employer owned files will copy to the user's personal devices and personal files of the employee will copy back to the employer owned computer's signed in to the account. This risk is exacerbated by the fact that many

applications (such as Dropbox) will automatically continue to synchronise back and forth without the end user necessarily realising that he / she is continuously placing new data on employer owned devices.

3.4.1.9 Management of cookies and search history

Mobile Device Management (MDM) software are often used by employers to monitor employees' personal device usage which invades on employees' privacy (Kabanda & Brown, 2014: 2). Logical access controls such as usernames and passwords are used to protect personal information. Bruwer (2013: 21) argues that Web 3.0 has the ability to organise information and integrates different datasets in order to generate new information. Digital history can now be attached to user profiles and no longer merely relates to devices. This technology has made target advertising possible. Internet search history is saved on the cloud to allow target advertising regardless of the device used to access the internet.

User history is built from search history, social media profiles, geographic location and other internet activity of the specific user linked to the user profile. This whole history influences the user experience and is accessible to any device as soon as the user profile is successfully signed in to. Many applications also request access to other applications to share data with each other. Google and Facebook accounts are often used by other applications to extract contacts and popular searches. A user with a smartphone might link his Gmail and Facebook accounts to share contacts. If that user access his Gmail account from a work computer and allows a work email or office management application, such as Microsoft Outlook, to access and share data with the Gmail account, the user's Facebook friends list will synchronise to the work mail through the Gmail account. The risk arises that personal information of employees may unknowingly synchronise to employer's databases and personal user accounts may influence user's experiences of the internet in the workplace. Liquid computing results in every user having a unique experience of the internet, which is counterproductive.

3.4.1.10 Invasion of employee personal time

Cloud computing, mobility, BYOD and consequently liquid computing has the major common advantage of increasing productivity. Employees' productive time is no longer limited to the office and meetings can be scheduled, e-mails answered or forwarded and information can be shared from any device with internet connectivity (Kabanda & Brown, 2014: 2). This has created a culture where it has become the norm for customers and clients to expect service after normal office hours. A potential problem identified by Comisky and Diamond (2014: 391) is the dilemma regarding overtime work since workers using their own devices after hours for work related matters might expect to be remunerated for overtime. Overtime and inappropriate use are not the only risks identified by Comisky and Diamond. They argue that there is also a health and safety risk posed by employees who are not able to step away from mobile devices used to perform their work such as answering e-mails whilst driving (Comisky & Diamond, 2014: 393). These increased office hours result in increased stress and decreased staff morale which might ultimately lead to decreased productivity. Liquid computing poses a risk to the human capital of organisations as employee morale may be negatively affected.

3.4.2 Risks pertaining to integrity of data

Liquid computing is the seamless switching between devices with no loss of processing ability or functionality. The experience can only truly be liquid, if all devices offer the same level of functionality. Different operating systems, network speeds and processing capabilities result in specific applications developed to optimise performance of devices. When these devices communicate with different protocols, interface between the protocols enable communication (Passerone *et al.*, 1998: 9). There is a risk that data may be corrupted, changed or lost amongst all these levels of translation and retrofitting. This risk is further increased by autonomous synchronisation. In a truly liquid environment, the user would not have to manually initiate synchronisation. The user grants permission for the initial synchronisation and further sessions of synchronisation is initiated either on fixed time intervals, whenever data changes or whenever connected to a network. These result in

data being overridden, deleted and added without the user specifically authorising the particular session.

3.4.2.1 Overwriting legitimate data

Seamless mobility and constant synchronisation results in constant updating of master data (Wikman, 2015: 4). Users work on several devices at different locations simultaneously in a liquid environment. All devices update to and from the central database to ensure users are working with accurate and relevant information. These updates are not limited to office hours since users are not limited to their offices. Slow or intermittent connectivity, resulting in outdated and erroneous data on user devices, might result in double entries or inaccurate processing by a user. These inaccuracies synchronising back to the server, will result in overwriting of legitimate data on the server.

3.4.2.2 Synchronisation conflict management

Synchronisation failure might have the consequence of obsolete information delivery to users which will result in inappropriate decisions. According to Filemaker (2010), there are five key issues pertaining to synchronisation to consider:

- **Database structure similarity.** The more similar in structure, the less complex the synchronisation will be. Synchronisation will be very complex with numerous possible pitfalls in the event of multiple databases with multiple structural differences.
- **The frequency of synchronisation.** High frequency synchronisation will lead to a higher need for processing power and more powerful hardware.
- **Resolution of data conflict.** How situations will be resolved where more than one of the datasets have been modified since the last synchronisation. Possible issues to consider here will be whether a specific dataset or user changes will receive preference or if the system will log conflicts and allow users to choose which option to synchronise to all datasets in the system.
- **Budget available to develop synchronisation system.** More complex synchronisation systems will require more expensive hardware and software

and as a result, the system will inevitably be limited by available financial resources.

- **Effort willing to invest in each synchronisation session.** This issue relates to whether the organisation wants synchronisation to happen autonomously and without user intervention or even without users realising that synchronisation is taking place, or whether the organisation is willing and able to invest employee time and effort into the synchronisation process thus trading productive time for this administrative task. Automatic synchronisation without any user intervention might result in a more user-friendly experience and more productive employee time, but this type of synchronisation bears much higher risk and thus will be more complex and need a much higher capital investment in hardware and software. This issue is thus closely related to the financial resources available.

These five key issues identified by FileMaker, result from the offline use of data using various different mobile computing devices. The data is then altered on the individual devices and once the device is connected to the network or internet, these changes to data need to reflect on the server of the organisation and also push the changes to all other connected devices. If a device is thus used offline, the central data is not updated in real time and multiple users might be updating their own versions of the downloaded data at the same time. Once all of these users' devices are connected again and synchronised, problems might possibly arise as the different users' data is now synchronised to the centralised datacentre. Wikman (2015: 4) identified that digital collaboration results in updates to the same document from more than one device at a time. This could result in incomplete or duplication of updates. The server will have to decide how these synchronisation conflicts will be managed.

3.4.2.3 Connectivity failure during synchronisation

Sarker and wells identifies network capabilities as an inhibitor in the use and adoption of mobile device adoption (Sarker & Wells, 2003: 37). In Sub-Saharan Africa, network coverage is limited. Internet speed is slow and connectivity is

unreliable. This gives rise to the risk of incomplete synchronisation. Large datasets need fast and reliable internet connections in order to synchronise. Connectivity failure amidst a synchronisation session could potentially corrupt data. In a truly liquid environment, the user signs in with a user profile and synchronisation initiates automatically. The risk arises that a synchronisation session initiates during an intermittent period of good connectivity and is carried out incompletely when connectivity is lost. If these instances are not logged properly, synchronisation cannot resume to complete the session once connectivity is restored.

3.4.2.4 Malicious software

Smartphones and tablets are vulnerable to malicious software such as viruses, Trojan horses and ransomware (Samaras *et al.*, 2014: 1). COBIT 5 requires enterprises to ensure the security in endpoints (ISACA, 2012a: 159). Securing endpoints entails security measures to protect the endpoints physically and logically. Individuals' devices are specifically vulnerable to logical security attacks such as those posed by ransomware. Mobile devices are used on a variety of networks, since the attractiveness of a mobile device is its ability to connect anywhere. The ability to connect to different networks increases the risk of ransomware on mobile devices. A major disadvantage of applications is that developers of applications usually have no information about users' security requirements (Armando *et al.*, 2014: 49). The developers will typically focus on viruses and common malware when developing applications, ignoring the fact that trusted applications can become entry points for security violations (Armando *et al.*, 2014: 49). In order to seamlessly switch between mobile devices and desktop solutions, the user has to log in to his profile and authorise the mobile device to access the network. During a synchronisation session, all files will be replicated from the device to the server and back from the server to the device. This replication will result in any malicious software on the device being copied to the server. Users might constantly be copying malware onto their employer's servers without knowing it with every synchronisation session.

3.4.2.5 Unapproved software and data manipulation

Liquid computing offers seamless switching and mobility to different devices. Various applications are developed to accommodate different operating systems and platforms (Zhang & Adipat, 2005: 294). Users are constantly searching for applications with more ease of use and functionality (Zhang & Adipat, 2005: 295). Several different applications are developed to perform essentially the same tasks, with differences in layout and interface to suit personal preference. Users might be working on the same data on different applications. The same user might opt to use a different application on a mobile device to continue a task started on another application on a desktop. This switching of information between devices and applications could result in processing differences and data corruption. Users and employers also have no control over the testing of applications and different application stores have varying levels of testing standards before allowing an application to be offered to its users. Untested applications or applications with insufficient security measures may be used by users on personal devices to work on very sensitive data. This places the data owner (the employer) at risk, not only for a loss of data, but also for the corruption of data. Data corruption might be intentional and malicious, but it may also occur inadvertently as a result of data having to constantly switch between applications and different protocols.

3.4.2.6 Lack of support

Sahd (2015: 52, 2016) identifies that insufficient IT support is a risk regularly manifesting itself in enterprises deploying mobile solutions. Application development is a lucrative business and programmers are constantly developing applications to address needs of users. Applications developed by large enterprises are generally deemed safer since large organisations do not want to risk reputational damage and therefore test applications extensively before launch. Smaller application developers do not have the resources to perform extensive stress tests. There is also a risk that these developers do not have the resources to provide support. Users might download an application because of its user-friendly interface (Scarfo, 2012: 447). Sufficient application support can help to recover data and provide patches in the event of application

bugs and crashes. Without support organisations may lose data completely or suffer from data corruption.

3.4.2.7 Discontinued applications

The success of an application is dependent on a number of non-functional factors (Wasserman, 2010: 3). Restrictions of mobile devices that also need to be considered when developing applications are (Wasserman, 2010: 1–4):

- Application behaviour when connected using a telephone network as opposed to being connected using a WiFi or WiMax connection. Differences in security and responsiveness are to be considered as well as if the higher likelihood of intermittent connectivity requires additional mechanisms.
- Techniques needed to ensure data integrity. Risks to data integrity include loss of connectivity or battery failure during synchronisation and updating.
- Speed dependency of applications and whether applications should be designed differently depending on the speed of the network.
- Battery life and resource usage should be maximized since applications are designed to be used on various mobile devices with different battery life and computational power.

Applications are regularly updated by developers. The risk arises that users might not choose to update their applications and miss out on security patches. Updating applications could also result in bugs or viruses finding a point of entry onto a device (and consequently the network) through an update. Applications not deemed to be viable are often discontinued. Users might download and use applications that could be discontinued at any stage. Users do not have control over data storage on application servers. Instant messaging applications might save all conversations without the users having any control over it. Once an application is discontinued, the servers that were used to run the application, might be sold or used for new or alternative applications. COBIT 5 suggests that endpoint devices should be disposed of securely (ISACA, 2012a: 159). Enterprises replacing servers have policies and procedures in place to ensure all data is removed from old servers. Depending on the security-consciousness of the organisation, varying levels of controls will be implemented to limit this

risk. These controls cannot be enforced on application servers to ensure deletion of data from discontinued application's servers.

3.4.2.8 Interoperability

The premise of a liquid computing environment is that any task can be handed off between different devices with seamless mobility. Users use their own personal devices and handoff tasks between mobile devices and computers. Device purchase is based on personal preference and financial means. The risk arises that data might be communicated by protocols that are not compatible. Mobile technology has a limited reach due to limitations in capability to communicate across networks and these limitations hamper adoption of the technology (Sarker & Wells, 2003: 35–40). Interoperability is the ability of different devices to communicate and collaborate without data corruption or loss of functionality (Wikman, 2015: 1). In a liquid environment, with many different users and devices, the risk of interoperability threatens the integrity of data.

3.4.2.9 Limited functionality

One of the key challenges for the deployment of wireless internet infrastructure is to efficiently manage user mobility (Banerjee *et al.*, 2003: 54–61). The original design of the internet does not appropriately address mobility since seamless use of mobile devices is a problem when relying on Internet protocol (Maier, Mühlbauer, Rogoza & Feldmann, 2007: 136–137). Liquid computing requires seamless switching between different devices (Desruelle, Isenberg, Lyle & Gielen, 2013: 5). In a truly liquid computer environment, all functionality is retained regardless of the device (Desruelle *et al.*, 2013: 5). Different processing capabilities and network speeds of devices and connections might limit functionality across different devices or applications. This argument is supported by Zhang and Adipat (2005: 293–308) who found that applications for mobile devices are limited by the computational power and memory capacity of mobile devices which still lags behind those of desktop computers. Snoeren *et al.* (2001: 34–41) argue that the internet lacks general support for mobile operation. Mobile applications are specifically designed, developed and

installed to address many of the problems associated with mobility. Applications are often developed with minimised functionality compared to their website counterparts, in order to decrease data cost and battery usage and increase speed. Many mobile internet systems are difficult to use and lack flexibility and robustness (Buchanan, Farrant, Jones, Harold, Marsden & Pazzani 2001: 673–680). Mobile internet websites used to have reduced functionality to accommodate mobile devices which have smaller screens and less processing power than conventional computers. Snoeren *et al*. (2001: 34–41) identified the following five fundamental issues raised by mobility:

- Location
- Preservation of communication
- Disconnection handling
- Hibernation
- Reconnection

In order to enable less powerful devices, the functionality and thus the liquidity of the computer environment is limited.

3.4.2.10 Battery failure

Mobile devices are used in liquid computing environments. Computing tasks started on conventional desktops or laptops, can seamlessly be continued on mobile devices. Mobile devices are dependent on batteries. Battery performance is severely affected by the processing power and specific use of the device (Kang, Park, Seo, Choi & Hong, 2008: 532). Powerful processors and constant connectivity drains batteries. Kang, Park, Seo, Choi and Hong (2008: 531) argue short battery life is a factor that reduces usefulness of mobile devices and causes much inconvenience to its users. Battery failure during synchronisation sessions will interrupt synchronisation. As with network connection, without logging, data corruption or loss might occur if synchronisation sessions are interrupted (Wasserman, 2010: 3).

3.4.3 Other risks

The most disruptive risks pertaining to liquid computing relates to the privacy and integrity of data. A few additional risks can also be identified:

3.4.3.1 Uncontrollable cost

Liquid computing relies on constant synchronisation of data between all devices. Large databases need to be downloaded and updated constantly. The cost of mobile data is still very high in South Africa, as is the case with all developing countries (Alfreds, 2016). Users without access to uncapped internet connections can accumulate high internet costs as a result of constant synchronisation. Once user profiles are linked to devices, these synchronisations will happen automatically between different devices, using the cloud as intermediary, without the user realising that data is being downloaded and uploaded (Marshall & Tang, 2012: 546). Employers that expect employees to use personal devices to increase efficiency, could potentially see employees trying to recover the cost of data from them. Smaller enterprises might not have uncapped internet access and might also experience running out of data and overrunning data budgets.

3.4.3.2 Slow network speed

Poor network coverage, lack of reliability and reduced responsiveness of the network are factors that impacts negatively on users' adoption of mobile technology (Sarker & Wells, 2003: 35–40). Fast internet connectivity is a necessary requirement for using applications that are dependent on the internet (Sharad, 2014). Apart from big metropoles, access to fast internet in South Africa is very limited. Internet service providers throttle internet users because of the limited availability of internet connection and speed. Slow internet speed is a limiting factor on liquid computing as this technology requires constant synchronisation over all devices and some applications require high speed connections (Schilit, Theimer & Welch, 1995: 1). Great differences in internet speed of two users might lead to inaccuracies and frustration where both are working on the same data at the same time, as there will be a significantly longer lead time on the side of the user with the slower connection. This might

also lead to incomplete synchronisation sessions and possible corruption of data.

3.4.3.3 Internet access

Azizi and Hashim found that availability of information should be safeguarded as information is a key asset for the business (Azizi & Hashim, 2010: 334). Digital divide is the disparity between the members of a population with access to computers and the internet and those who do not (Van Dijk, 2006: 223). According to Statistics South Africa, less than 10% of South Africans have access to the internet at home (Statistics South Africa, 2015). Smartphones and cellular contracts provide access to a great part of the population, but the high cost of mobile data limits the usage of mobile devices for internet access. This hampers the adoption of liquid computing since individuals do not synchronise company information and applications to personal devices. Wherever a strategy of liquid computing is utilised, it must be done with the supposition that it is a bonus but not a given. This point of departure can only be deviated from, if the company provides internet access to all who might have to use its data and information. Corporates often provide data sims and mobile internet routers to employees to increase internet availability.

Limited access to internet and the high cost of mobile data limits the adoption of liquid computing to those with unrestricted access to internet as all synchronisation across devices need internet access.

3.4.3.4 Litigation

Enterprises utilise controls to ensure data privacy and confidentiality. The enterprise can only manage the security of data hosted on devices and networks over which it has control. Comisky and Diamond argue that employees may be harassed or communicate inappropriately with their own devices which might lead to company liability if the company utilises a BYOD policy and the device is also associated with the entity (Comisky & Diamond, 2014: 387). In Sahd's investigation into the mobile solutions, the author identified that enterprises are at risk of possible litigation from employees for

the loss of personal information (Sahd, 2015: 58, 2016). Autonomous synchronisation also results in customers' and clients' confidential information being delivered to private devices of employees. This constitutes a loss of control over data and information. Once data is synchronised to employee-owned devices, the enterprise can no longer guarantee the security and confidentiality of the data. Samaras, Daskapan, Ahmad and Ray argues that customers and business partners of the enterprise will hold the enterprise accountable in the event of a confidentiality breach and that companies are still legally bound to implement security over data privacy (Samaras *et al.*, 2014: 3).

3.5 Risks mapped to COBIT

The IT Gap is a result of a hap-hazard, ad-hoc approach to risk management. For the purposes of this research, a control framework has been used to follow a structured approach in identifying risks incremental to liquid computing. COBIT Version 5 has been chosen as a framework. The control processes listed in COBIT were summarised in Table 3 below. All the identified risks are also indicated on the table by an X. After studying the literature on these risks as well as COBIT, each risk was mapped to the relevant processes of COBIT. Some of the risks relates to how users will use the technology whereas other risks relate to the technology design itself. User behaviour will map very strongly to the "Monitor, evaluate and assess domain", as the entity will have to monitor that users use the technology responsibly. The risks concerning the technology itself, will map many of the processes in the Build, acquire and implement domain as the technology and network architecture will have a direct impact on these risks:

Table 3 Risk mapping to COBIT

		Risks																							
Domain	Processes	Loss of control over information	Device theft	Device disposal	Unauthorised device access	Accidental espionage	Accidental disclosure	Interception during communication	Loss of personal information	Cookies and search history	Invasion of employee personal time	Overriding data	Sync conflict management	Connectivity failure	Malicious software	Unapproved software	Lack of support	Discontinued applications	Interoperability	Limited functionality	Battery failure	Uncontrollable cost	Slow network speed	Internet access	Litigation
Evaluate, direct and monitor	Ensure governance, framework setting and maintenance	X		X	X	X	X		X	X					X	X	X	X	X						
	Ensure benefits delivery	X										X	X	X		X	X	X	X	X	X	X	X	X	
	Ensure risk optimisation	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
	Ensure resource optimisation	X						X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	
	Ensure stakeholder transparency		X	X	X	X	X		X	X	X														X

(Continued on next page)

		Risks																							
Domain	Processes	Loss of control over information	Device theft	Device disposal	Unauthorised device access	Accidental espionage	Accidental disclosure	Interception during communication	Loss of personal information	Cookies and search history	Invasion of employee personal time	Overriding data	Sync conflict management	Connectivity failure	Malicious software	Unapproved software	Lack of support	Discontinued applications	Interoperability	Limited functionality	Battery failure	Uncontrollable cost	Slow network speed	Internet access	Litigation
Align, plan and organise	Manage the IT management framework	X		X	X	X	X		X	X					X	X	X	X	X						
	Manage strategy	X						X		X		X	X	X	X	X	X		X						X
	Manage enterprise architecture		X	X	X			X		X	X	X	X	X	X	X			X	X					
	Manage innovation	X						X	X	X	X	X	X	X	X	X		X	X	X					
	Manage portfolio	X						X				X	X	X	X	X	X	X	X	X					
	Manage budget and costs																X	X				X	X	X	
	Manage human resources		X	X	X	X	X	X	X	X	X														
	Manage relationships								X	X	X							X							
	Manage service agreements	X											X	X	X		X	X	X	X			X	X	
	Manage suppliers	X											X	X	X		X	X	X	X			X	X	
	Manage quality	X											X	X	X	X	X	X		X					
	Manage risk	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
	Manage security		X	X	X	X	X	X							X										

(Continued on next page)

		Risks																							
Domain	Processes	Loss of control over information	Device theft	Device disposal	Unauthorised device access	Accidental espionage	Accidental disclosure	Interception during communication	Loss of personal information	Cookies and search history	Invasion of employee personal time	Overriding data	Sync conflict management	Connectivity failure	Malicious software	Unapproved software	Lack of support	Discontinued applications	Interoperability	Limited functionality	Battery failure	Uncontrollable cost	Slow network speed	Internet access	Litigation
Build, acquire and implement	Manage programmes and projects	X							X	X	X	X	X	X	X	X	X	X	X	X					
	Manage requirements definition	X										X	X	X	X	X	X	X	X	X	X		X	X	
	Manage solutions identification and build	X								X	X	X	X	X	X	X	X	X	X	X			X		
	Manage availability and capacity											X	X	X			X	X	X	X	X	X	X	X	
	Manage organisational change enablement	X						X	X	X	X	X	X	X	X	X	X	X	X	X				X	X
	Manage changes	X						X	X	X	X	X	X	X	X	X	X	X	X	X				X	X
	Manage change acceptance and transitioning	X	X	X	X	X	X	X	X	X	X					X	X	X						X	
	Manage knowledge	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X						X
	Manage assets	X	X	X	X	X	X	X				X	X	X	X	X	X	X	X	X	X				
	Manage configuration	X						X	X	X	X	X	X	X					X	X			X		

(Continued on next page)

		Risks																						
	Processes	Loss of control over information	Device theft	Device disposal	Unauthorised device access	Accidental espionage	Accidental disclosure	Interception during communication	Loss of personal information	Cookies and search history	Invasion of employee personal time	Overriding data	Sync conflict management	Connectivity failure	Malicious software	Unapproved software	Lack of support	Discontinued applications	Interoperability	Limited functionality	Battery failure	Uncontrollable cost	Slow network speed	Internet access	Litigation
Deliver, service and support	Manage operations	X						X	X	X	X	X	X	X	X	X	X	X	X	X	X		X	X	
	Manage service requests and incidents		X				X	X	X	X	X		X	X			X			X			X	X	X
	Manage problems	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
	Manage continuity	X										X	X	X	X	X	X	X							X
	Manage security services	X													X	X									
	Manage business process controls	X	X	X	X	X	X		X	X	X					X	X	X							

(Continued on next page)

		Risks																						
	Processes	Loss of control over information	Device theft	Device disposal	Unauthorised device access	Accidental espionage	Accidental disclosure	Interception during communication	Loss of personal information	Cookies and search history	Invasion of employee personal time	Overriding data	Sync conflict management	Connectivity failure	Malicious software	Unapproved software	Lack of support	Discontinued applications	Interoperability	Limited functionality	Battery failure	Uncontrollable cost	Slow network speed	Internet access	Litigation
Monitor, evaluate and assess	Monitor, evaluate and assess performance and conformance	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X			X	X	
	Monitor, evaluate and assess the system of internal control	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X								
	Monitor, evaluate and assess compliance with external requirements	X	X	X	X	X	X	X	X	X	X					X										X

(Source: Author's own)

3.6 Risk matrix

Risk management entails the identification and quantification of risks. Risks should be ranked based on the quantification in order to prioritise controls to be implemented. Risks can be separated into two elements in order to quantify them. The more likely a risk is to occur, the bigger the risk is to the organisation. The other element of risk quantification is the severity of the impact on the organisation if the risk does occur (ISACA, 2012b: 116).

Risks to liquid computing have been identified in the previous section. The likelihood of each of the risks to occur, is assigned a rating of one (1) to five (5) on a Likert scale as follows:

1. Very unlikely to occur.
2. Unlikely to occur.
3. Possibility of risk occurrence.
4. Likely to occur.
5. Very likely to occur.

The severity of the risks' impact on the organisation in the event of occurrence will be rated as follows:

1. No disruption to operations, might cause inefficiencies.
2. Some disruption to operations, might lead to some reputational damage.
3. Severe disruption to operations, will definitely lead to reputational damage, might cause business failure.

The risks identified in Table 3, were listed in Table 4 below. Each of these risks were quantified based on their likelihood to occur on a scale of one (1) to five (5) and the impact on the organisation on a scale of one (1) to three (3) should these risks occur. Judgement has to be exercised in scoring these risks. In order to illustrate the risk matrix, a generic organisation was used. A risk that is most likely to occur (5) that would severely disrupt operations and cause reputational damage (3), would score rating of 15 (5X3). Risks that are highly unlikely to occur (1) and would cause no disruptions and only minor inefficiencies (1), would obtain a scoring of 1 (1X1). It is important to note that this table is only presented here for illustrative purposes of the risk matrix and each organisation would have to perform the scoring of risks since the impact of each risk, in particular, on a specific organisation would depend on the type of data managed by the organisation. Many of the risks incremental to liquid computing relate to the privacy of data. A medical aid scheme or bank will contain much more sensitive details than a grocery franchise.

Risks of one to five (1 – 5) would be accepted as low risk. A risk with a rating of six to ten (6 – 10) is deemed medium risk. Any risk with a rating that exceeds ten (10), is deemed a high risk and unacceptable. It is imperative to the continuation of the business that these risks be mitigated by means of controls.

Table 4 Quantification of risks

Risk	Likelihood [A]	Impact [B]	Risk rating [A*B]
Risk of loss of control over information	4	2	**8**
Risk of device theft	3	2	**6**
Device disposal	5	2	**10**
Risk of unauthorised access to devices	4	2	**8**
Accidental espionage	3	2	**6**
Accidental disclosure	4	2	**8**
Risk of interception of information during communication	4	2	**8**
Loss of personal information of users	4	1	**4**
Management of cookies and search history	4	1	**4**
Invasion of employee personal time	4	2	**8**
Overwriting legitimate data	4	3	**12**
Synchronisation conflict management	4	3	**12**
Connectivity failure during synchronisation	4	3	**12**

(Continued on next page)

Risk	Likelihood (1 – 5) [A]	Impact (1 – 3) [B]	Risk rating [A*B]
Malicious software	4	3	**12**
Unapproved software and data manipulation	4	3	**12**
Lack of support	4	3	**12**
Discontinued applications	4	3	**12**
Interoperability	5	3	**15**
Limited functionality	4	2	**8**
Battery failure	5	3	**15**
Uncontrollable cost	4	1	**4**
Slow network speed	5	1	**5**
Internet access	5	1	**5**
Litigation	2	3	**6**

(Source: Author's own)

The maximum quantification a risk can obtain is fifteen (15). That would mean that a risk is most likely to occur (5) and the impact of such a risk on the enterprise would be devastating (3). Risks of interoperability and battery failure obtained the maximum rating of fifteen (15). These risks are sure to occur (5) and, in the event that the occurrence of these events lead to an incomplete synchronisation session or the corruption of data, this might cause severe disruption to an organisation (3). The lowest risk is that of uncontrollable cost. Most large enterprises utilising a liquid computing strategy, would have uncapped internet at the office. The cost of data to the employees would be for the employees own account or, in the event of employer-supplied data, only a fixed amount of data would be supplied. The impact of this risk on the enterprise, is therefore negligible.

3.7 Conclusion

Any new technology results in new risks for an organisation. Liquid computing gives rise mainly to risks relating to privacy and integrity of data. The risks have been identified by using a structured approach of an existing control framework. The control framework's detailed processes were tabled and the risks were mapped to these processes in Table 3. Those risks were carried over to Table 4, where each of these risks were quantified.

The risks were ranked based on their likelihood to occur and the potential impact on the organisation. From Table 4 the conclusion can be drawn that the areas of highest risk pertain to battery failure during synchronisation (15), interoperability (15) and integrity breaches due to synchronisation issues and malicious software (12). The areas of lowest risk to the organisation are the risks of internet access (5), slow networks (5) and uncontrollable cost of data (4).

It is important to note that the severity of the impact of the risk will depend on the sensitivity of data in the organisation's possession. The ranking provided in this chapter is a guideline, but each organisation should perform this ranking process on its own risks taking into account the sensitivity of its data. This ranking is done without taking any controls into consideration. The next chapter will recommend possible controls to mitigate these risks.

Chapter 4 – Controls for an environment of liquid computing

4.1 Introduction

Internal controls should be implemented at various levels in order to mitigate risk (Rudman, 2010: 3253). Orman states that reduction of risk should be a major concern (Orman, 2013: 23). The previous chapter identified risks associated with liquid computing. A control framework was used to follow a structured approach in identifying these risks. These risks were then quantified based on their likelihood to occur and the impact on an organisation in the event of occurrence.

The aim of this chapter is to identify controls to mitigate the risks identified in the previous chapter. Controls will be quantified based on their ability to prevent the risk from occurring and their ability to limit the impact of risks. A thorough understanding of the technologies enabling liquid computing was obtained in Chapter 2. This understanding, together with COBIT 5 and ISO 2700 series, which address IT security, will aid in the identification of controls. Risks with a higher risk rating, need more and stronger controls in order to sufficiently mitigate it to an acceptable level.

4.2 Controls

Effective control and security of IT can increase an organisation's competitive position, customer satisfaction, staff morale, productivity, reputation, sales and profitability (Symons, 2005: 59). The list below contains suggested controls to address the risks identified in the previous chapter. These controls were identified by performing an extensive literature review on the enabling technologies, COBIT 5 and the ISO 2700 series and this does not present an exhaustive list of possible controls. Technology is constantly changing and consequently the risks pertaining to technology also consistently changes. This list should be used as a starting point, but each enterprise should identify risks based on the specific organisational structure, technological architecture and operational environment.

4.2.1 Information security policies

Enterprises should govern liquid computing by means of scripted policies. The board needs to direct management of the technology and employees should be educated on the policy upon employment (Sahd, 2015: 62). Acceptable behaviour and use of resources should be clearly communicated and employees should sign the policy. The policy should contain disciplinary procedures and these should be followed without exception when employees are in breach of the policy. Clearly communicated policies that are understood by users prevent unacceptable behaviour and disciplinary action upon breach of policies deters users from breach in future.

4.2.2 Continuous training

Employees should be trained to understand the dangers and consequences of liquid computing. Employees will be more conscious of their actions if they understand the dangers and risks associated with the technology (Sahd, 2015: 64). Updates on training should continuously be provided and compulsory sessions should be scheduled to prevent employees from becoming indifferent to the risks as well as update them on newly identified risks.

4.2.3 Risk reporting

Hardy feels the board should insist that risk management forms part of the operations of an enterprise and that quick reporting and response is imperative to managing risk (Hardy, 2006: 56). Reporting hotlines should be established for users to report breach of liquid computing security policies. These hotlines should be attended to at all times and incidences such as lost or stolen devices should immediately be logged. The affected device can then be remotely wiped and immediately unauthorised and locked out of the system to prevent any synchronisation to and from the device in question.

4.2.4 Encryption

Sahd states that data encryption should be used for all data stored on the cloud or communicated over the internet (Sahd, 2015: 72). Authorised devices contain encryption keys that can decrypt the data to a readable format. This data will be unreadable whilst being communicated over unsecured and public networks. This control provides a layer of protection against interception.

4.2.5 Data segregation

Data segregation is also known as data containerisation (Sahd, 2015: 73). This control technique separates sensitive data from less sensitive data. Sensitive data is never synchronised and downloaded to any device. The technique protects the privacy of data, but limits the liquidity of the computing environment as this control will consequently result in functionality being lost for mobile devices.

4.2.6 Remote wipe

This is a technique whereby all corporate data can be wiped from a stolen or lost device remotely (Sahd, 2015: 72). Scarfo also found that this technique easily allows full control on applications that have access to data and thus devices can be remotely locked and data wiped (Scarfo, 2012: 450). This control technique is only useful if the user informs the enterprise timeously that the device has been lost or stolen.

4.2.7 Data fading

Sahd suggests that this control is helpful in a mobile environment as it will automatically delete data after a specific lapse of time from a disconnected device (Sahd, 2015: 72). This control technique limits loss of data, but uses a lot of data as the device has to synchronise all data once a valid connection is established again.

4.2.8 Thin client models

In a thin client model, data is not downloaded to the device but rather stored and managed centrally (Sahd, 2015: 73). The device contains no data and thus data is kept private, however, as with data fading, this control technique necessitates the synchronisation of all data for every valid connection session which may increase processing time and will increase data cost.

4.2.9 User profiles

Sahd suggests that usernames and passwords in conjunction with one time passwords be used to ensure only authorised access to data (Sahd, 2015: 72). Applications should log out users after inactivity and require passwords upon a request to reopen the application. Banking applications utilise this control to protect mobile device users' bank accounts from unauthorised access. If the device is lost or stolen, the password is required to reconnect. Different users will be assigned different access rights and, when used in conjunction with data segregation, this control technique can limit access to sensitive data for junior employees altogether (Samaras *et al.*, 2014: 3).

4.2.10 Availability testing

This control attempts to address the availability of battery power and the availability of network connectivity.

Neugebauer and McAuley suggests that energy, like any other resource, can be managed in mobile computing devices (Neugebauer & McAuley, 2001: 63). Applications should require a predefined minimum battery lifetime for the application to open, process, save and synchronise. Once the remaining battery life of a device falls below the predefined level, the application should not permit the user to open it, or process further in events where the application was opened prior to battery drainage. Android operating system already employs this feature for the camera application (Paksoft Tools, 2011).

The same principle applying to battery life, can be used to test network availability prior to synchronisation. Data-heavy synchronisation should not

automatically initiate over mobile data or when slow or intermittent network connectivity is detected. This will prevent synchronisation sessions from being interrupted because of insufficient mobile data or loss of connectivity. Data saved locally should only be deleted once the synchronisation session is completed successfully.

4.2.11 Synchronisation conflict management

Farrow found that continuous monitoring of synchronisation quality is not feasible (Farrow, 2006: 333). Farrow suggests that synchronisation quality falling below a predefined acceptable margin should be reported to the server with a snapshot of the time interval error data, centred around the time of the occurrence (Farrow, 2006: 332). A proper synchronisation system, should update the central data with all the users' changes and the central datacentre should provide accurate and timeous information. This updated and accurate central datacentre should then synchronise back to the different devices connected to the network in order to ensure that all devices contain the latest and accurate information. The system should thus only recognise the changes made by each individual user and only synchronise those changes (and not the whole database) from the user device back to the system. This approach will prevent a scenario where a user who worked offline connects to the network and the database on that user's device overwrites the whole database on the network, deleting all the updates from other users made earlier. Many synchronisation systems requires manual intervention for all synchronisation conflicts. In the event of multiple devices updating the same line item, the event should be logged and the incident reported to all involved devices. All the attempted synchronisations should be saved and users prompted to manually resolve it in order to prevent double processing or processing omissions.

4.2.12 Activity logs

Activity logs and time stamps are important to limit and reverse the consequences of security and integrity breaches (Wikman, 2015: 4). Clock setting and synchronisation between servers and devices are important in an environment with various devices communicating to a central database (Calder,

2008; Self, 2013). Synchronisation interruptions and errors should be time stamped. Wikman suggests document versions and indexing to limit loss of data during interruptions (Wikman, 2015: 4). This suggested model of Wikman will save data with version and time stamp information and index these files to improve efficiency during recovery (Wikman, 2015: 4). Backups prior to synchronisation sessions can provide recovery data for failed synchronisation attempts. Once connectivity is restored, the synchronisation session should be restarted.

4.2.13 Standardised protocols

According to Turner, Budgen and Brereton, a lack of a single, standardised language of communication is a factor limiting the success of the SaaS model (Turner *et al.*, 2003: 42). Protocol standardisation ensures reliable communication between networks and devices. A protocol interface, translating different protocols, helps to overcome the issue of inadequate protocol standardisation (Passerone *et al.*, 1998: 9). Communication differences are especially apparent in mobile solutions between devices operating on iOS, Windows Mobile and Android platforms. SyncML (Synchronous Mark Up Language) is a common language for synchronising all devices over any network, minimising bandwidth and dealing with the low reliability and high network latency of wireless networks (Lee *et al.*, 2002: 133). A standardised communication protocol prevents data corruption and can ensure seamless transition of data and information between devices.

4.2.14 Preferred suppliers

COBIT suggests that trusted mechanisms should be allowed to support transmission and receipt of data (ISACA, 2012a: 159). Organisations should only allow data to synchronise to trusted applications. A list of trusted applications should continuously be updated and accessible to all employees. This control technique will provide a degree of quality control as the organisation can choose to only use applications that underwent vigorous testing and were developed by reputable developers with whom the organisation can establish partnerships. Enterprises can also opt to develop their own applications to take

control over security employed by the application. Common security features that should be coded into applications are, but not limited to:

- Restrict download of sensitive data,
- Employ user profiles in conjunction with an access control matrix,
- Enforce strong passwords,
- Automatic sign out after set periods of inactivity,
- Encryption, and
- Remote termination of device's access to application.

Service level agreements with cloud based service providers and SaaS contracts can also be entered into to ensure quality and availability. Public clouds are made available to the public in a pay-as-you-go manner while private clouds refer to internal datacentres of an organisation that are not made available to the public (Armbrust *et al.*, 2009: 10). Organisations can thus utilise private clouds to increase mobile access to its data resources. Preferred hardware might be provided to employees, but this option will require significant capital investment and increases risks related to asset management.

4.2.14 Anti-malware

Bruwer suggests that anti-malware software be installed to eliminate the threat of malicious software (Bruwer, 2013: 50). Sahd also argues that anti-virus software should not only be installed, but also regularly updated (Sahd, 2015: 72). Networks in liquid environments should have the latest versions of anti-malware installed to protect it against malware synchronised from other devices. Anti-malware for mobile operating systems are not commonly used yet, but employees registering devices on the employer's network should be required to have anti-malware installed on all devices that synchronise to the organisational network. Firewalls and virtual private networks with powerful and extensive anti-virus software is imperative to the protection of the corporate network.

An expensive option is to develop the architecture of the network to protect the primary server from communication with mobile devices. This can be achieved by placing an intermediary server between the primary server and the various

mobile devices. The intermediate server would synchronise to and from the devices and on a fixed timed interval. After a successful sweep of the intermediary server by anti-malware, the intermediate server would terminate connections to other devices and synchronise to the primary server. Once this synchronisation is completed, connection to the primary server should be terminated and connection to mobile devices can resume. Figure 2 below illustrates this architecture. The order in which actions are initiated and completed is indicated by the numerical values:

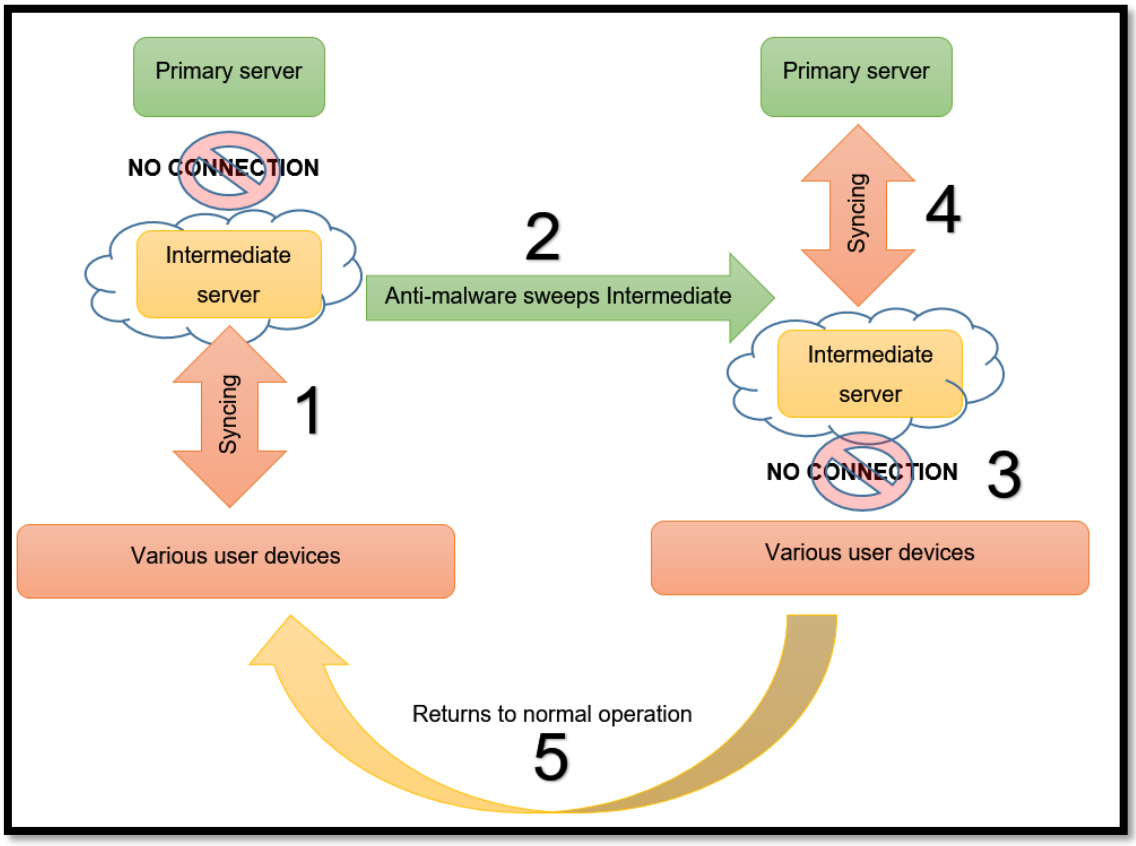

Figure 2 The intermediate server model

(Source: Author's own)

4.3 Control matrix

During a risk management process, risks are quantified and prioritised. Suggested controls should also be quantified based on their ability to mitigate risk. Organisations should use stronger and more controls to mitigate higher areas of risk. Controls were quantified based on their ability to identify / highlight the occurrence of a risk (notification) as well as the ability of the control to contain the impact of the risk on an organisation (containment). These controls can either be preventative or detective. Preventative controls (proactive) will not prevent a specific risk from threatening an organisation while a detective control (reactive) will identify a risk that has occurred and enable the organisation to limit the consequences. Both preventative and detective controls have various abilities to notify management of the risk event in a timely fashion, as well as various abilities to contain the impact of the risk on the organisation. Controls are quantified on a Likert scale from one to five based on their ability to notify management of the risk situation threatening an organisation as follows:

1. Highly unlikely to highlight risk to management / Not able to notify management timely of possible risk.
2. Unlikely to notify risk to management timeously.
3. Might notify management of risk, depending on situation. Not always timeous.
4. Likely to notify management of risk timeously.
5. Most likely to notify management of risk in a timely manner in all situations.

The ability of a control to contain the impact of a risk that has already occurred and, is quantified from one to three as follows:

1. Unlikely to contain consequences of risk timeously.
2. May contain consequences of risk.
3. Likely to contain consequences of risk timeously.

An element of judgement is needed when quantifying controls. The specific design and implementation of a control would impact the quantification awarded to a control. Each organisation would have to perform this quantification based on the strength of the control for that specific organisation. The quantification

awarded in Table 5 below is generic to illustrate the working of the matrix. A control that is most likely to notify management timeously of a risk occurrence (5) and likely to contain the consequences of the risk in a timeous manner (3), will obtain a quantification of 15 (5 X 3). Controls that are highly unlikely to notify management of a risk occurrence timeously (1) and unlikely to contain the consequences of the risk in a timeous manner (1), will obtain a quantification of 1 (1 X 1). The controls discussed in the preceding section were tabled in Table 5 below and quantified as follows:

Table 5 Quantification of controls

Control	Notification (1-5) [D]	Containment (1-3) [E]	Control rating [D*E]
Information security policies	3	1	**3**
Continuous training	3	1	**3**
Risk reporting	3	3	**9**
Encryption	4	1	**4**
Data segregation	4	1	**4**
Remote wipe	1	3	**3**
Data fading	2	2	**4**
Thin client models	5	1	**5**
User profiles	3	1	**3**
Availability testing	4	1	**4**
Synchronisation management	4	2	**8**
Activity logs	1	2	**2**
Standardised protocols	5	1	**5**
Preferred suppliers	4	1	**4**
Anti-malware	4	1	**4**

(Source: Author's own)

From Table 5 above, it can be seen that risk reporting, which can be used by employees to report lost or stolen devices or devices infected with malware, immediately, obtained the highest quantification. This was a result of this control scoring three (3) out of possible five (5) on its ability to notify management of a compromise in data and a three (3) out of possible three (3) on the ability to contain the consequences of this risk. However, this rating only holds as long as the reporting line is accessible at any hour and the device can then immediately be blocked from the network. Should the reporting line only be available during office hours, or the device cannot be remotely locked, the strength of this control is severely compromised. For this reason, each organisation should quantify their specific controls based on the design and implementation of the controls in that specific organisation. The IT department can assist in the quantification of the controls, since their knowledge about network architecture and the technology itself, would assist in determining how strong the control would be and under which circumstances the control would be overridden. Other controls scoring strongly, were synchronisation management (8), thin client models (5) and standardised protocols (5), which ensures that data is not corrupted during synchronisation sessions, not stored on user's devices and can be communicated between different devices, respectively.

4.4 Conclusion

The controls suggested in this chapter does not represent an exhaustive list of controls and implementing these controls cannot guarantee mitigation of all risks pertaining to liquid computing. The aim of this study was to investigate the technology in order to identify the risks that are incremental to continuous synchronisation and to recommend controls to mitigate these identified risks.

From Table 5 it can be seen that the most effective control would be to establish a reporting channel where employees can immediately report security breaches on personal devices which would enable the organisation to de-authorise the device in question from the network. Other very important controls, as from the

matrix in Table 5, are to ensure that data is not stored on employee's devices, standardising protocols to ensure communication between different devices and synchronisation management software that will prevent data corruption during synchronisation sessions.

The next chapter summarises the findings and concludes with a mapping of the controls to the risks in order to indicate which risks are addressed by which controls. The quantification of controls are deducted from the relevant risk quantifications in order to quantify whether the unmitigated risk remaining after implementation of the controls, are acceptable.

Chapter 5 - Conclusion

5.1 Overall findings of the study

The Millennial generation is now entering the labour market. This generation has never known an era without hyper-connectivity. Devices are connected to networks and data is synchronised to and from devices and networks on a continuous basis. This constant synchronisation of devices, has led to an era where the computing experience of a specific user can seamlessly hand-off from one device to another. This seamless mobility has given rise to risks for businesses. This study aids management of businesses to identify the risks incremental to liquid computing, suggests possible controls to mitigate these risks and quantifies the unmitigated, remaining risk after implementation of the suggested controls.

In order to understand the risks and controls incremental to liquid computing, the term had to be defined. Chapter 2 of this study identified the components that are present in a liquid computing environment. These components include hardware, software and enabling technologies. A literature study was conducted on the enabling technologies in order to better understand liquid computing. The common characteristics present in a liquid computing environment were identified and liquid computing was defined as a scalable state of computing where all devices are constantly updated with data from the datacentre and the computing experience is seamlessly handed off between devices connected to the network.

Chapter 3 identified the risks incremental to liquid computing. Risk cannot be identified on an ad-hoc basis and a control framework was studied to identify the risks. COBIT Version 5 was used for this purpose. The risks were all mapped to the detailed processes of COBIT in Table 3. This table indicates how the risks relates to the processes. The risks identified in Table 3 were then carried over to Table 4 to be quantified. In Table 4, each risk was awarded a risk quantification based on its likelihood to occur and the severity of the impact the risk would have on the organisation. The biggest risks identified, are all related

to interruption during synchronisation or malicious software, resulting in a possible compromise in data integrity and possible leak of sensitive information.

Chapter 4 suggests controls for the risks identified in Chapter 3. COBIT 5 and the ISO 2700 series standards were studied in order to suggest controls for each of the risks identified. Table 5 lists these controls and quantifies them based on their success rate in notifying management of the risk (notification) and the ability to contain the consequences in the event that a risk did occur (containment). The most effective controls identified in Table 5 are controls related to reporting security breaches immediately (which addresses risks relating to how users utilise the technology), and management of synchronisation sessions in order to prevent compromise in the integrity of data during synchronisation conflicts or interruptions.

Table 6 below maps the suggested controls (as taken from Table 5) to the risks (as taken from Table 4) it addresses. An “X” indicates that a risk is addressed by the control in the corresponding column. The unmitigated risk (the risk that remains for an organisation that implements the suggested control) is calculated by subtracting the control quantification from the risk quantification. Some risks are addressed by more than one control in order to build redundancy into the proposed control environment. In these instances, all the relevant control quantifications were subtracted from the risk quantification to calculate the unmitigated risk. The unmitigated risk is limited to a minimum quantification of one (1) since no risk can be completely mitigated by controls, regardless of the strength of the control(s). A score of one to five (1 – 5) is deemed to be low risk, six to ten (6 – 10) is deemed to be medium risk and a score of eleven to fifteen (11 – 15) indicates a high risk. High or medium unmitigated risk is not acceptable and alternative measures should be investigated to further mitigate the risk.

Table 6 Unmitigated risk after implementing suggested controls

			Controls															
			Information security policies	Continuous training	Risk reporting	Encryption	Data segregation	Remote wipe	Data fading	Thin client models	User profiles	Availability testing	Synchronisation management	Activity logs	Standardised protocols	Preferred suppliers	Anti-malware	UNMITIGATED RISK
		Quantification	3	3	9	4	4	3	4	5	3	4	6	2	5	4	4	
Risks	Risk of loss of control over information	8	X	X	X													1
	Risk of device theft	6	X		X		X	X	X	X	X							1
	Device disposal	10	X				X	X	X	X	X							1
	Risk of unauthorised access to devices	8	X	X			X			X	X							1
	Accidental espionage	6	X	X														1
	Accidental disclosure	8	X	X	X	X					X					X		1
	Risk of interception of information during communication	8	X	X		X	X						X			X	X	1
	Loss of personal information of users	4	X	X			X									X		1

(Continued on next page)

			Controls															
			Information security policies	Continuous training	Risk reporting	Encryption	Data segregation	Remote wipe	Data fading	Thin client models	User profiles	Availability testing	Synchronisation management	Activity logs	Standardised protocols	Preferred suppliers	Anti-malware	UNMITIGATED RISK
		Quantification	3	3	9	4	4	3	4	5	3	4	6	2	5	4	4	
Risks	Management of cookies and search history	4	X	X												X		1
	Invasion of employee personal time	8	X	X			X									X		1
	Overwriting legitimate data	12	X										X	X				1
	Synchronisation conflict management	12	X										X	X				1
	Connectivity failure during synchronisation	12	X									X	X	X				1
	Malicious software	12	X	X												X	X	1
	Unapproved software and data manipulation	12	X	X		X										X		1
	Lack of support	12	X													X		5
	Discontinued applications	12	X													X		5
	Interoperability	15	X												X	X		3

(Continued on next page)

			Controls															
			Information security policies	Continuous training	Risk reporting	Encryption	Data segregation	Remote wipe	Data fading	Thin client models	User profiles	Availability testing	Synchronisation management	Activity logs	Standardised protocols	Preferred suppliers	Anti-malware	UNMITIGATED RISK
		Quantification	**3**	**3**	**9**	**4**	**4**	**3**	**4**	**5**	**3**	**4**	**6**	**2**	**5**	**4**	**4**	
Risks	**Limited functionality**	**8**	X													X		**1**
	Battery failure	**15**	X									X	X	X				**1**
	Uncontrollable cost	**4**	X										X					**1**
	Slow network speed	**5**	X									X	X					**1**
	Internet access	5	X										X					**1**
	Litigation	6	X	X		X	X		X									**1**

(Source: Author's own)

From Table 6 above it can be concluded that none of the risks identified in this study remains at medium or high level after implementation of the proposed controls. The highest unmitigated risk observed from Table 6, is an unmitigated risk quantification of five (5). This is an acceptable unmitigated risk as any risk between one and five is deemed to be low. The risks obtaining an unmitigated risk quantification of five (5) were risks relating to lack of support and discontinued applications. The risk pertaining to interoperability scored an unmitigated risk quantification of three (3). All the other risks scored a quantification of one (1) after implementation of all the suggested controls.

5.2 Critique of the study and its contributions

The recommendations of this study are based on generic risks related to the technology of liquid computing. The risks pertaining to this technology can be classified into risks pertaining to the privacy of data and risks pertaining to the integrity of data. Risk quantification therefore depends on the type of data contained on an enterprise's servers. The risk and control quantification models developed and used in this study can thus be used as a starting point, but each organisation should reperform the quantifications based on its own information assets and control environment. This study also only deals with the risks incremental to liquid computing and is by no means an exhaustive list of all risks and controls pertaining to an enterprise utilising the enabling technologies. It is also important to bear in mind that technologies and the way they are used are constantly changing. Sophistication of hackers and malicious software are constantly increasing. The list of possible risks (and therefore also the controls) should therefore be continuously updated.

5.3 Recommendations for further research

Controls were suggested based on the incremental risks identified. The controls are only suggested on a high level and further research is necessary to suggest how these controls can be implemented on an operational level. The technical details regarding the information systems architecture and protocol

standardisation and interface that will manage synchronisation conflicts should be studied further to assist with seamless adoption of this technology.

The matrix used to quantify risks and controls in this study, is based on a very generic organisation. This quantification of the individual risks and controls would have to be adjusted for each specific organisation. Further research needs to be conducted to study the impact of the risks and proposed controls on specific industries. Management's input is imperative to quantifying the risks and similarly, IT professionals' input would be invaluable in the quantification of the controls of a specific organisation. When used correctly, this matrix could assist in bridging the IT Gap in organisations as it breaks down the mitigation of risk into sections understood by management and IT professionals, respectively. The matrix should be tested in practice.

References

Aker, J.C. & Mbiti, I.M. 2010. Mobile Phones and Economic Development in Africa Working Paper 211 June 2010 Mobile Phones and Economic Development in Africa. *Center for Global Development*. (June 2010):1–44.

Alfreds, D. 2016. *Here's why SA data prices won't come down soon*. [Online], Available: http://www.fin24.com/Tech/News/heres-why-sa-data-prices-wont-come-down-soon-20160215 [2016, October 19].

Armando, A., Costa, G., Verderame, L. & Merlo, A. 2014. Securing the "Bring your own device" paradigm. *Computer*. 47(6):48–56.

Armbrust, M., Fox, A., Griffith, R., Joseph, A.D., Katz, R., Konwinski, A., Lee, G., Patterson, D., et al. 2009. *Above the Clouds: A Berkeley View of Cloud Computing*. (UCB/EECS-2009-28). California. [Online], Available: http://radlab.cs.berkeley.edu/ [2015, August 15].

Ayyash, M., Elgala, H., Khreishah, A., Jungnickel, V., Little, T., Shao, S., Rahaim, M., Schulz, D., et al. 2016. Coexistence of WiFi and LiFi Toward 5G : Concepts , Opportunities , and Challenges. *IEEE Communications Magazine*. 54(2):64–71.

Azizi, N. & Hashim, K. 2010. Enterprise level IT risks: An assessment framework and tool. In *Proceedings - 2010 3rd IEEE International Conference on Computer Science and Information Technology, ICCSIT 2010*. Vol. 3. Beijing, China. 333–336.

Bai, C.E., Liu, Q., Lu, J., Song, F.M. & Zhang, J. 2004. Corporate governance and market valuation in China. *Journal of Comparative Economics*. 32(4):599–616.

Banerjee, N., Wu, W., Das, S.K., Dawkins, S. & Pathak, J. 2003. Mobility Support in Wireless Internet. *IEEE Wireless Communications*. 10(5):54–61.

Basson, B. 2014. The right to privacy : How the proposed POPI Bill will impact data security in a Cloud Computing environment - Presented in partial fulfilment of the requirements for the degree Masters of Commerce (Computer Auditing). Stellenbosch University.

Bradley, R. & Pratt, R. 2011. Exploring the Relationships among Corporate Entrepreneurship, IT Governance, and Risk Management. In *44th Hawaii International Conference on System Sciences*. Hawaii, USA. 1–10.

Bruwer, H.J. 2013. An Investigation of Developments in Web 3.0: Opportunities, Risks, Safeguards and Governance - Presented in partial fulfilment of the requirements for the degree Masters of Commerce (Computer Auditing). Stellenbosch University.

Bruwer, R. & Rudman, R. 2015. Web 3.0: Governance, Risks and Safeguards. *Journal of Applied Business Research*. 31(3):1037.

Buchanan, G., Farrant, S., Jones, M., Thimbleby, H., Marsden, G. & Pazzani, M. Improving mobile internet usability. In *Proceedings of the tenth international conference on World Wide Web - WWW '01*. Hong Kong, China. 673–680.

Buyya, R., Yeo, C.S., Venugopal, S., Broberg, J. & Brandic, I. 2009. Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. *Future Generation Computer Systems*. 25(6):1–17.

Calder, A. 2008. *ISO27001 / a Pocket Guide*. Second edi ed. Ely: IT Governance Publishing. [Online], Available: http://www.books24x7.com/marc.asp?bookid=58240. [2015, October 30].

CCM. 2016. *What is WiFi and How Does it Work ?* [Online], Available: http://ccm.net/faq/298-what-is-wifi-and-how-does-it-work#q=What+is+WiFi+and+How+Does+it+Work?&cur=1&url=/ [2016, October 09].

Chaffey, D. 2015. *Insights from KPCB US and global internet trends 2015*. [Online], Available: http://www.smartinsights.com/internet-marketing-statistics/insights-from-kpcb-us-and-global-internet-trends-2015-report/ [2015, July 07].

Christensen, C.M. 1997. *Innovator ' s Dilemma*. Boston, Massachusetts: Harvard Business School. [Online], Available: http://www.biznews.com/wp-content/uploads/2013/04/the_innovators_dilemma.pdf [2015, July 06].

Cisco. n.d. *What is a Network Switch vs. a Router?* [Online], Available: http://www.cisco.com/cisco/web/solutions/small_business/resource_center/articles/connect_employees_and_offices/what_is_a_network_switch/index.html?referring_site=smartnavRD [2016, July 04].

Comisky, H.A. & Diamond, T.E. 2014. *The Risks and Rewards of a BYOD Program: Ensuring Corporate Compliance without causing "Bring Your Own Disaster" at Work*. (Report). Charleston: Charleston School of Law.

Desruelle, H., Isenberg, S., Lyle, J. & Gielen, F. 2013. Multi-device application middleware: Leveraging the ubiquity of the Web with webinos. *Journal of Supercomputing*. 66(1):4–20.

Van Dijk, J.A.G.M. 2006. Digital divide research, achievements and shortcomings. *Poetics*. 34(4–5):221–235.

Farrow, C. 2006. Recent advances in continuous on-line synchronisation testing for telecom networks. In *Proceedings of the IEEE International Frequency Control Symposium and Exposition*. Geneva, Sitzerland. 331–333.

FileMaker. 2010. *Database synchronisation - an overview of approached*. [Online], Available: http://help.filemaker.com/app/answers/detail/a_id/7720/~/database-synchronization---an-overview-of-approaches [2016, June 17].

Fomin, V. V, De Vries, H.J. & Barlette, Y. 2016. ISO / IEC 27001 Information Systems Security Management Standard : Exploring the reasons for low adoption. In *Third European Conference of Management of Technology*. Paris, France.

Friedhoff, J.M. & Mansouri, M. 2016. A Framework for Assessing Technology Risks in Transaction-Based Extended Enterprises: U.S. Capital Market Case. *IEEE Systems Journal*. 1–11.

Gartner. 2016. *Gartner's IT Glossary*. [Online], Available: http://www.gartner.com/it-glossary/ [2016, June 20].

Goralski, W. 2009. *The Illustrated Network*. Burlington: Morgan Kaufmann Publishers.

Grose, C., Theodoros, K. & Chouliaras, V. 2014. Corporate Governance in Practice. The Greek Case. *Procedia Economics and Finance*. 9(Ebeec 2013):369–379.

Hardy, G. 2006. Using IT governance and COBIT to deliver value with IT and respond to legal, regulatory and compliance challenges. *Information Security Technical Report*. 11(1):55–61.

Hartman, J., Manber, U. & Peterson, L. 1996. *Liquid software: A new paradigm for networked systems*. Tucson. [Online], Available: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.49.3549&rep=rep1&type=pdf\npapers2://publication/uuid/03F2D625-4E26-4283-ADC4-80E659711C66.

Hoffman, C. 2015. *What is the Difference between a Modem and a Router*. [Online], Available: http://www.howtogeek.com/234233/whats-the-difference-between-a-modem-and-a-router/ [2016, July 14].

Imazeki, J. 2014. Bring-Your-Own-Device: Turning Cell Phones into Forces for Good. *The Journal of Economic Education*. 45(3):240–250.

Institute of Directors Southern Africa (IODSA). 2009. *King Code of Governance for South Africa*. [Online], Available: https://jutalaw.co.za/uploads/King_III_Report/#p=2 [2016, July 14].

ISACA. 2012a. *COBIT 5 Customized Process Reference Guide*. [Online], Available: http://www.isaca.org/COBIT/Pages/COBIT-5-Enabling-Processes-product-page.aspx [2015, October 10].

ISACA. 2012b. *A Business Framework for the Governance and Management of Enterprise IT*. [Online], Available: http://www.isaca.org/cobit/documents/cobit-5-introduction.pdf [2015, October 10].

IT Governance Institute (ITGI). 2003. *Board Briefing on IT Governance*. 2nd ed. [Online], Available: http://wikimp.mp.go.gov.br/twiki/pub/EstruturaOrganica/AreaMeio/Superintendencias/SINFO/Estrategia/BibliotecaVirtual/MaterialExtra/26904_Board_Briefing_final.pdf [2016, July 14].

Iyer, N. & Bonissone, P.P. 2007. Automated risk classification and outlier detection. In *Proceedings of the 2007 IEEE Symposium on Computational Intelligence in Multicriteria Decision Making, MCDM 2007*. Hawaii, USA. 272–279.

Kabanda, S. & Brown, I. 2014. Bring-Your-Own-Device (BYOD) practices in SMEs in Developing Countries – The Case of Tanzania. In *25th Australasian Conference on Information Systems*. Auckland, New Zealand. 1–9. [Online], Available: http://aut.researchgateway.ac.nz/bitstream/handle/10292/8153/acis20140_submission_149.pdf?sequence=1&isAllowed=y.

Kang, J.M., Park, C.K., Seo, S.S., Choi, M.J. & Hong, J.W.K. 2008. User-centric prediction for battery lifetime of mobile devices. In *11th Asia-Pacific Network Operations and Management Symposium1th Asia-Pacific Network Operations and Management Symposium*. Vol. 5297. Beijing, China: Springer Berlin Heidelberg. 531–534.

Kim, H.-W., Chan, H.C. & Gupta, S. 2007. Value-based Adoption of Mobile Internet: An empirical investigation. *Decision Support Systems*. 43(1):111–126.

Krechovská, M. & Procházková, P.T. 2014. Sustainability and its integration into corporate governance focusing on corporate performance management and reporting. *Procedia Engineering*. 69:1144–1151.

Lee, B., Kim, T., Kim, D. & National, C. 2002. Data synchronization protocol in mobile computing environment using yncML. In *5th IEEE International Conference on High Speed Networks and Multimedia Communication (Cat. No.02EX612)*. Jeju Island, Korea. 133–137.

Lenhart, A., Purcell, K., Smith, A. & Zickuhr, K. 2010. *Social Media & Mobile Internet Use Among Teens and Young Adults*. Washington D.C.

Maier, G., Mühlbauer, W., Rogoza, Y. & Feldmann, A. 2007. Enabling seamless mobility. In *Proceedings of the 2007 ACM CoNEXT conference*. Vol. 42. New York, USA. 136.

Marshall, C. & Tang, J.C. 2012. That syncing feeling: early user experiences

with the cloud. In *DIS '12 Proceedings of the Designing Interactive Systems Conference*. Newcastle, UK. 544–553.

Mikkonen, T. & Systä, K. 2014. Liquid Software Manifesto. In *IEEE 38th Annual International Computers, Software and Applications Conference*. Vasteras, Sweden. 338–343.

Narayan, S. & Gajski, D.D. 1995. Interfacing Incompatible Protocols using Interface Process Generation. In *32nd Conference on Design Automation*. San Francisco, USA.

Neugebauer, R. & McAuley, D. 2001. Energy is just another resource: Energy accounting and energy pricing in the Nemesis OS. In *Proceedings Eighth Workshop on Hot Topics in Operating Systems*. Elmau, Germany. 59–64.

Orman, L. V. 2013. Technology as risk. *IEEE Technology and Society Magazine*. 32(2):22–31.

Paksoft Tools. 2011. *Low Battery Camera*. [Online], Available: https://play.google.com/store/apps/details?id=thepaksoft.net.lowbatterycamera [2016, October 19].

Passerone, R., Rowson, J.A. & Sangiovanni-Vincentelli, A. 1998. Automatic Synthesis of Interfaces between Incompatible Protocols. In *35th Annual Design Automation Conference*. San Francisco, USA. 8–13.

Rudman, R.J. 2010. Framework to identify and manage risks in Web 2 . 0 applications. *African Journal of Business Management*. 4(13):3251–3264.

Sahd, L. 2015. A Structured Approach to the Idenfication of the Significant Risks Related to Enterprise Mobile Solutions at a Mobile Technology Component Level - Presented in partial fulfilment of the requirements for the degree Masters of Commerce (Computer Auditing). Stellenbosch University.

Sahd, L. 2016. Significant risks relating to mobile technology. *Journal of Economic and Financial Sciences*. 9(1):291–309.

Samaras, V., Daskapan, S., Ahmad, R. & Ray, S.K. 2014. An Enterprise Security Architecture for Accessing SaaS Cloud Services with BYOD. In *11th Australasian Telecommunication Networks and Applications Conference*. Melbourne, Australia. 1–6.

Sarker, S. & Wells, J.D. 2003. Understanding mobile handheld device use and adoption. *Communications of the ACM*. 46(12):35.

Satyanarayanan, M., Kozuch, M.A., Helfrich, C.J. & O'Hallaron, D.R. 2005. Towards seamless mobility on pervasive hardware. *Pervasive and Mobile Computing*. 1(2):157–189.

Scarfo, A. 2012. New security perspectives around BYOD. In *Proceedings - 2012 7th International Conference on Broadband, Wireless Computing, Communication and Applications, BWCCA 2012*. Victoria, Canada. 446–451.

Schilit, B.N., Theimer, M.M. & Welch, B.B. 1995. Customizing Mobile Applications. In *USENIX Symposium on Mobile & Location-independent Computing*. Cambridge, USA. 1–9.

Self, R. 2013. IS Practices for SME Success Series. In *IS Practices for SME Success Series*. Vol. 1. L. Mawhinney & R. Self, Eds. University of Derby. 1–148.

Sharad, S. 2014. Increasing internet speed and bandwidth by using laws of physics. In *Proceedings - 2014 International Conference on Intelligent Computing Applications, ICICA 2014*. Tamilnadu, India.

Singh, M.N. & Phil, M. 2012. B . Y . O . D . Genie Is Out Of the Bottle – " Devil Or Angel ". *Journal of Business Management & Social Sciences Research*. 1(3):1–12.

Smith, A. 2013. *Smartphone Ownership 2013*. (Report). Washington D.C.: Pew Research Center.

Snoeren, A.C., Balakrishan, H. & Kaashoek, M.F. 2001. Reconsidering Internet Mobility. In *Proceedings Eighth Workshop on Hot Topics in Operating Systems*. Elmau, Germany. 34–41.

Spremic, M. 2012. Corporate IT Risk Management model: A holistic view at managing information system security risks. In *Proceedings of the ITI 2012 34th International Conference on Informaiton Technology interfaces*. Cavtat, Croatia. 299–304.

Statistics South Africa. 2015. *Statistics SA: Interactive data*. [Online], Available: http://interactive.statssa.gov.za:8282/webview/ [2016, October 19].

Susanto, H., Almunawar, M.N. & Tuan, Y.C. 2011. Information Security Management System Standards : A Comparative Study of the Big Five. *International Journal of Electrical & Computer Sciences*. 11:23–29.

Symons, C. 2005. *IT Governance Framework*. [Online], Available: http://i.bnet.com/whitepapers/051103656300.pdf [2016, July 14].

Tanner, A. 2015. *Behind the Surge in Cross-Device Ad Targeting | MIT Technology Review*. [Online], Available: http://www.technologyreview.com/news/538731/how-ads-follow-you-from-phone-to-desktop-to-tablet/?utm_campaign=newsletters&utm_source=newsletter-weekly-mobile&utm_medium=email&utm_content=20150706 [2015, July 08].

Toth, G.. 1994. Software technology risk advisor. In *Proceedings KBSE '94. Ninth Knowledge-Based Software Engineering Conference*. Moterey, USA. 179–188.

Turner, M., Budgen, D. & Brereton, P. 2003. Turning software into a service. *Computer*. 36(10):38–44.

Ulrich, B., Discolo, A. & Alam, S. 2000. *Patent No. US006052735A*.

Wasserman, A.I. 2010. Software Engineering Issues for Mobile Application Development. *ACM Transactions on Information Systems*. 1–4.

Webb, P., Pollard, C. & Ridley, G. 2006. Attempting to define IT governance: Wisdom or folly? In *Proceedings of the 39th Annual Hawaii International Conference on System Sciences*. Vol. 8. Hawaii, USA. 1–10.

Wikman, J. 2015. EDB : A Multi-Master Database for Liquid Multi-Device Software. In *2015 2nd ACM International Conference on Mobile Software Engineering and Systems*. Florence, Italy: IEEE. [Online], Available: http://www.cs.tut.fi/~taivalsa/EDB-FullPaper-2014-09.pdf [2015, April 09].

Zhang, D. & Adipat, B. 2005. Challenges, Methodologies, and Issues in the Usability Testing of Mobile Applications. *International Journal of Human-Computer Interaction*. 18(3):293–308.